

Mobile Device Management

The only constant in mobility nowadays is change. Former market leaders such as RIM and Microsoft are now followers straining to keep pace with consumer-driven operating systems from Google and Apple. Almost **80%** say tablets will grow in importance. No two platforms have the same security and management hooks, yet your end users are demanding email, calendaring, VPN access and much more—**64%** are on board with custom apps. This is changing the face of computing—and terrifying the IT managers charged with providing productivity tools while maintaining control of sensitive data.

By Grant Moerschel



CONTENTS

TABLE OF

3

Author's Bio

4

Executive Summary

5

Research Synopsis

6

Rolling With the Changes

7

Impact Assessment

8

Productivity Is Power

9

Dodgy Application Behavior

10

Mobile Platform Trends

14

Mobile Apps

16

Mobile Device Policy

18

Security Control

20

Cohesive Management Via MDM

27

Appendix

41

Related Reports

Figures

6

Figure 1: Increase in Employee-Owned Mobile Devices?

8

Figure 2: Mobile Technology Impact on Productivity: 2010 vs. 2011

10

Figure 3: Lack of Access to Mobile Productivity Activities: Impact on Employees

11

Figure 4: Mobile Devices Selected by IT

12

Figure 5: Enterprise-Ready Mobile Platforms

13

Figure 6: Operating Systems Permitted to Access Business Resources

14

Figure 7: Custom Business Applications for Mobile Devices

15

Figure 8: Supported Mobile Platforms for Custom Applications

16

Figure 9: Use of Virtual Desktop Technologies Via Tablets

17

Figure 10: Mobile Device and Data Policies?

18

Figure 11: Enterprise Data Access Via Mobile Device: Default vs. Exception

19

Figure 12: Ability to Selectively Wipe Business Data From Personal Devices

20

Figure 13: Portable Device Security Controls

21

Figure 14: Primary Reason for Deploying MDM

22

Figure 15: Reasons for Not Deploying MDM

23

Figure 16: MDM Architecture

24

Figure 17: MDM Spending Plans

25

Figure 18: Access to Cloud Services Via Mobile Devices

27

Figure 19: Percentage of Employees Using Devices

28

Figure 20: Mobile Technology Impact on Productivity

29

Figure 21: Importance of Employee Access to Mobile Technologies

30

Figure 22: MDM Features of Interest

31

Figure 23: Types of Cloud Services Accessible Via Mobile Devices

32

Figure 24: Standardized on a Mobile Device Platform?

33

Figure 25: Carriers Selected by IT

34

Figure 26: Prioritization of Mobile Data Security

35

Figure 27: Portable Device Security Controls: 2010 vs. 2011

36

Figure 28: Mobile Device Management Vendors

37

Figure 29: Industry

38

Figure 30: Job Title

39

Figure 31: Company Revenue

40

Figure 32: Company Size

**Grant Moerschel***WaveGard*

Grant Moerschel is co-founder of WaveGard, a vendor-neutral technology security firm. His 22 years of IT experience encompass a wide range of strategic and tactical business technology functions, including significant experience with security engineering, mobility strategy, IT risk and vulnerability assessment, network engineering and wireless technology training. He has consulted for many clients, in both the public and private sectors. Grant is the co-author on the McGraw-Hill title *Certified Wireless Security Professional (CWSP) v2 Study Guide* and the Cisco Press title *CCSP Flash Cards and Exam Practice Pack*. In addition to being an Interop presenter, he has written numerous technical articles for *InformationWeek Reports* and courseware for (ISC)2. He earned his BS degree from the University of Delaware.

SUMMARY

EXECUTIVE

As you develop mobility policies, your ultimate goal should be the certainty that any data contained within a device, or any connectivity profiles—VPN or Wi-Fi—that provide access to corporate networks, is completely secure, even if the smartphone or tablet is lost or stolen. Can you look into an auditor’s eyes and say that with confidence?

Because the trend is toward personally owned devices, if an MDM system can’t differentiate between enterprise data and the owner’s data, don’t buy it. But this is just one in a long set of important, and nice to have, features. In general, candidate MDM platforms should support iOS and Android, with management links to RIM’s BES a big plus. It should be able to differentiate security capabilities by OS type, because not all operating systems are created equal. It should normalize controls regardless of platform, so IT doesn’t have to know the gory details. It should consume user-role data from centralized directory services so that changes that are fed from the central directory—including termination—affect the profile experience on the end device. Self-service functions, such as provisioning and bringing a device back into compliance after missteps like loading an app considered risky, help reduce the help desk load. In this report, we’ll examine trends in mobile device management and security and delve into policy development.

ABOUT US

InformationWeek Reports' analysts arm business technology decision-makers with real-world perspective based on qualitative and quantitative research, business and technology assessment and planning tools, and adoption best practices gleaned from experience. To contact us, write to managing director **Art Wittmann** at awittmann@techweb.com, content director **Lorna Garey** at lgarey@techweb.com, editor-at-large **Andrew Conry-Murray** at acmurray@techweb.com, and research managing editor **Heather Vallis** at hvallis@techweb.com. Find all of our reports at reports.informationweek.com

SYNOPSIS

RESEARCH

Survey Name *InformationWeek* Mobile Device Management and Security Survey

Survey Date August 2011

Region North America

Number of Respondents 323 respondents from companies with 50-plus employees involved with determining mobile/wireless strategy or evaluating, recommending or purchasing mobile devices.

Purpose This survey strives to gauge respondents' secure use of mobile computing technologies such as smartphones and tablets and the importance of the supporting security structure. By polling for trends in the overall use of mobile devices as well as the applications in use by respondents' organizations and their relative significance, it becomes clear which are the most mission-critical and would cause greatest disruption should they become unavailable. We also delve into the policy components governing the use of mobile technologies. Our aim is to determine the importance of mobile data protection to organizations, as well as whether mobile data policies are in place. On the tactical end, we asked about the most popular security controls being used, as well as centralized mobile device management systems and the rationale for seriously considering their use as a security control to enforce organizational mobile security policy.

Methodology *InformationWeek* surveyed business technology decision-makers at North American companies. The survey was conducted online, and respondents were recruited via an email invitation containing an embedded link to the survey. The email invitation was sent to qualified *InformationWeek* subscribers.

Rolling With the Changes

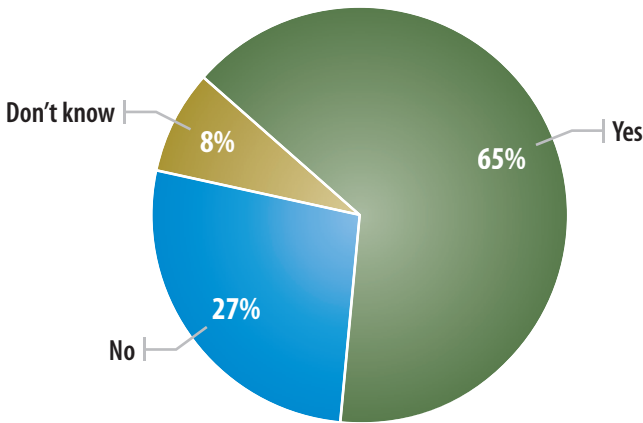
Judging from the 323 respondents to our *InformationWeek Reports Mobile Device Management and Security Survey*, all of whom are involved with determining mobile/wireless strategy or evaluating, recommending or purchasing mobile devices, the pace of change is accelerating. It's been 16 months since our last MDM research report, and in that time market shares have shifted considerably, fueled by alluring options from multiple vendors. Google's Android platform is rocketing up and has taken the lead from Research in Motion, which has been battered by outages.

Apple's growth remains level, even with the multitudes of new monthly activations. Palm's WebOS got a stay of execution when Palm was acquired by Hewlett-Packard but was terminated anyway—poof. And Nokia, rumored to be a takeover target, is moving at breakneck speed to dump Symbian in favor of Windows Phone. Microsoft itself is chugging along in the background, looking to reinvent and reinvigorate with a new end device strategy centered

Figure 1

Increase in Employee-Owned Mobile Devices?

Do you predict an increase in the percentage of employee-owned (a.k.a. "employee liable") smartphones and tablets accessing business resources? This implies a reduction of business-supplied devices.



Data: *InformationWeek 2011 Mobile Device Management and Security Survey* of 323 business technology professionals, August 2011

R3321011/14

on Windows 8, Windows Phone and the Metro GUI interface.

So many choices, so little time, says the IT manager. It's exciting, but also extremely challenging for those charged with aiding worker productivity while maintaining data security

and compliance. What IT needs is a solid mobility plan comprising four main areas:

- > **A policy** that describes how mobile devices are to be used in the environment
- > **Security controls** to be placed on devices, based on risk

- > **Procedures** for provisioning, managing and disposing of devices
- > **Systems** that enable us to manage both company- and employee-owned devices

It's been widely written, and we agree, that employee-owned devices are the future and that fewer IT organizations are defining and supplying a "preferred" platform. When IT can dictate, the choice is usually BlackBerry; the reasons stem from the fact that Android and iOS were designed from the ground up

with the consumer in mind, not corporations. As we discuss in our recent *InformationWeek Reports* IT Pro Ranking on smartphone and tablet operating systems, platform "fun factor" is the driving force behind consumer adoption vs. manageability and security being high on IT's list.

Regardless of whether these newer platforms are "open" (Android), "walled garden" (Apple) or somewhere in between, they are

Our data shows that smartphones generally held steady in terms of perceived importance, with laptops and netbooks trending down.

Impact Assessment: Mobile Device Management

| Impact to ... | Benefit | Risk |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IT Organization | ●●●●● By crafting a solid plan for supporting the operations and security of mobile devices, IT can save time and ensure consistent applications and security commensurate with mobility policy. | ○●●●● The risk of not offering consistent mobile apps is that lines of business will find a way to do it themselves, resulting in disarray and fragmentation. |
| Business Organization | ○●●●● Devices that are consistently configured provide a predictable working environment for users. | ●●●●● The risk of losing control of sensitive information has numerous legal, competitive, compliance and goodwill downsides. |
| Business Competitiveness | ●●●●● Employees armed with the organization's key communication functions and standard apps will be productive and happy. | ○●●●● Though lack of ability to work remotely is not necessarily a complete showstopper, it will become more important over time from both a retention and a competitive standpoint as the practice becomes more the norm. |
| Bottom Line: ○●●●●○●●●● | | |
| Our overall opinion on how to handle mobility security hasn't changed appreciably since our 2010 report. In this short 16 months, platforms have quickly evolved, as have the third-party tools used to manage them. IT must take the lead to identify a mobility strategy, have it accepted by leadership, and use one or two flexible management controls that enforce policies across the most popular phone and tablet types. Doing otherwise places organizational data in jeopardy. | | |

slicker and more fun, and the average person is adopting them fast. Thus consumerization is pushing platform popularity.

Whether it's because of shrinking budgets, the fact that employees now have capable

personal devices or a combination of the two, companies aren't supplying phones like they did in the past—a striking 65% of our respondents predict an increase in the percentage of employee-owned smartphones and tablets

accessing business resources.

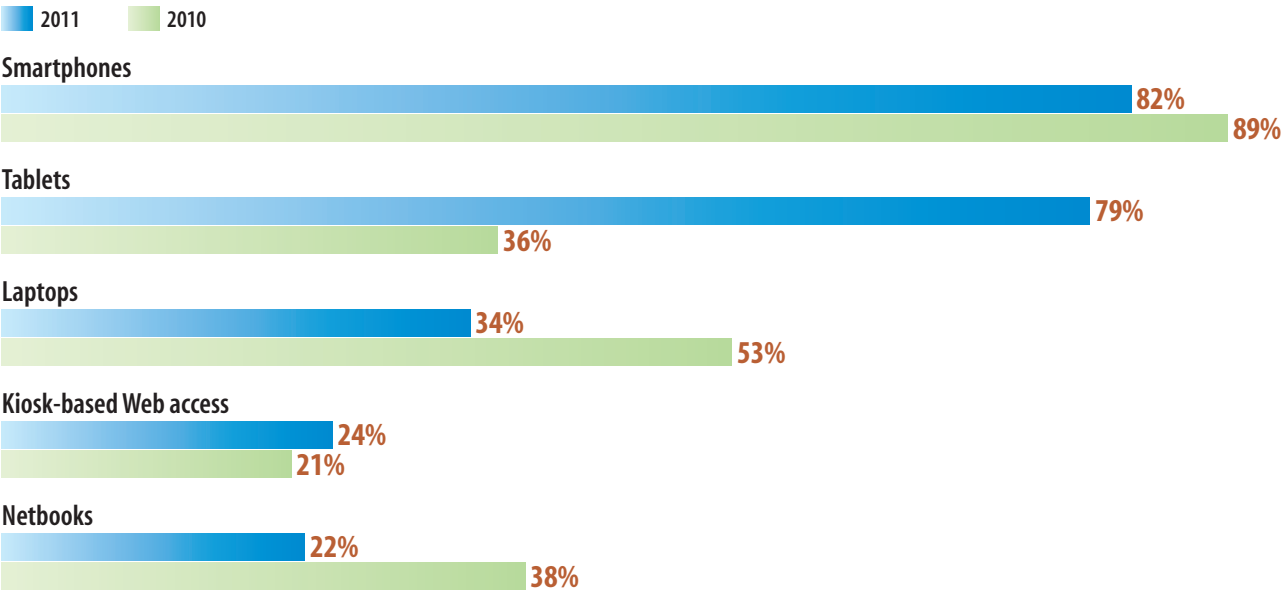
Since it's pretty clear that IT will be defining the hardware standard less often, we need to be prepared to support the plurality of platforms. That means policies and procedures defining how the fine line between what's yours and what's the company's will be managed and secured. In our opinion, the MDM platforms that will win customers are the ones that can manage Android, iOS and Windows Phone with links into RIM's BES. These MDM systems will be able to take advantage of each platform's inherent cryptographic capabilities and push operational security policies and profiles. They will detect risky security events, perform provisioning of digital certificates for encryption and authentication, and allow for the easy loading of private apps. They'll assist with control of sensitive information and data loss prevention.

And to top off that list, we believe one of the most important things a successful MDM system offers is deprovisioning, where enterprise apps, data, certificates and profiles are selectively wiped from the personal device

Figure 2

Mobile Technology Impact on Productivity: 2010 vs. 2011

Thinking about the next 24 months, how critical a role will the following mobile technologies play in business productivity at your company?



Note: Percentages reflect a response of “increase significantly in importance” or “increase somewhat in importance”
Base: 323 respondents in August 2011 and 307 in March 2010
Data: InformationWeek Mobile Device Management and Security Survey of business technology professionals

R3321011/3

in the event of an employee's departure. Enterprise data control must co-exist with the preservation of personal files on employee-liable devices, and IT needs the tools to make this a reality.

Productivity Is Power

Mobile technologies such as smartphones and tablets are playing a bigger role in business productivity because our definition of work continues to morph and spread beyond

office walls. “Smartphone technology has enabled our company to perform better and communicate easier through various channels,” says one respondent. “It has been less costly to use smartphones rather than laptops or desktops to communicate with employees, customers and vendors.”

This viewpoint extends to tablets, which nearly 80% of August 2011 respondents say will increase in importance within their organizations in the next 24 months, compared with just 36% saying the same in March 2010.

Just look around any airport and you’ll see the future. Granted, laptops can do more and still are the mobile standard for serious quantities of work, but perhaps the 80/20 rule applies here. With tablets, people can check their email, hit the Web and, if so enabled, do a quick virtual desktop or RDP session back to corporate via the built-in VPN. Often, that’s good enough.

Our data shows that smartphones generally held steady in terms of perceived importance, with laptops and netbooks trending down. We predict that netbooks will phase out, with

MOBILITY & RISK

Dodgy Application Behavior

At our May 2011 Interop Las Vegas session, “Securely Equipping a Mobile Workforce,” Michael Davis, CEO of Savid Technologies, and I presented a strategy for those seeking to reduce mobility platform risks, whether malicious or inadvertent. The “Top 10 Mobile App Risks” list that follows is designed to educate developers and security professionals about mobile application behavior that puts users and data at risk. Use it to determine the coverage of a mobile security system during app development and acceptance, app store white- and blacklisting determination, and when evaluating security software and MDM systems for a mobile platform.

Malicious Functionality

- > Unauthorized activity monitoring
- > Unauthorized dialing, SMS and payments
- > Unauthorized network connectivity (ex-filtration or command & control)
- > UI impersonation
- > System mods (rooting/jailbreaking)
- > Logic or time bomb

Vulnerabilities

- > Sensitive-data leakage (inadvertent or side channel)
- > Storage of sensitive data without encryption
- > Sensitive-data transmission without encryption
- > Hardcoded passwords/keys in apps

people choosing tablets instead. All the while, new development initiatives, like Intel’s Ultra-book technology, will challenge the tablet form factor when introduced.

All of this keeps us on our toes.

Road warriors can be a demanding lot, and their views on what’s important haven’t changed appreciably. Email/calendaring is still

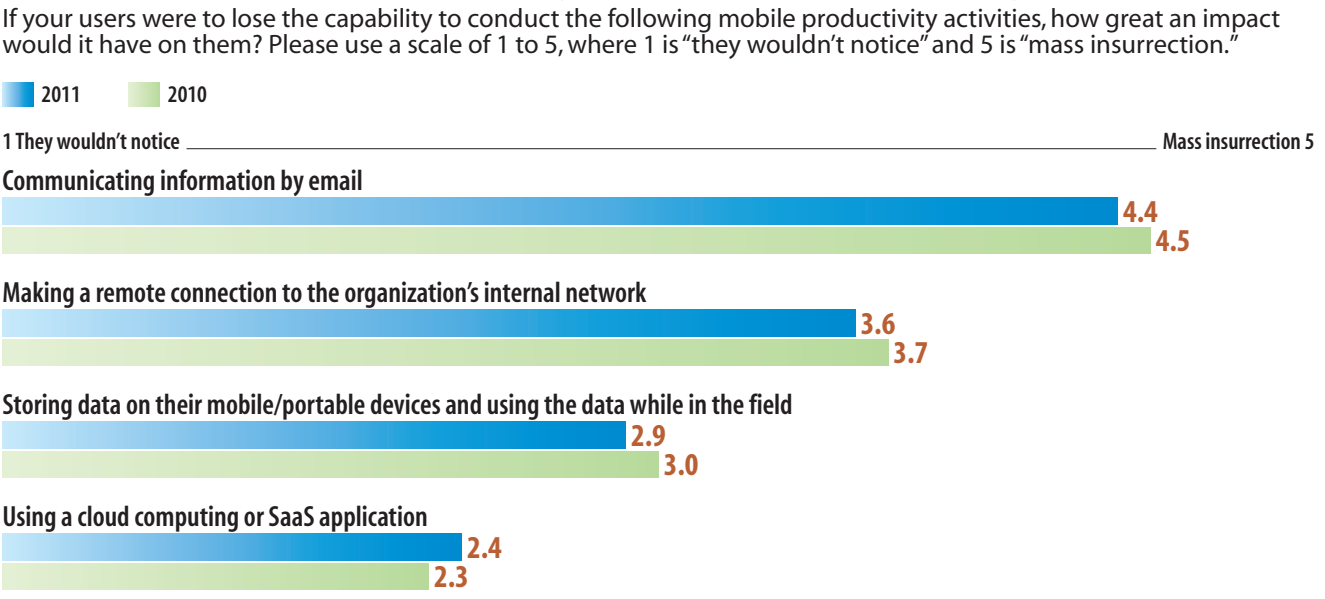
king, followed by plain-old Web access. However, application development and remote access technologies for mobile are quickly maturing. Software as a service is also getting more play. So look for these mobile-centric applications to take on more prominence with workers. Remember, the name of this game for IT is to deftly manage the component pieces—email profiles, internal and SaaS apps, whatever—making it easy for people to work but also having the confidence to look an auditor in the eye and say you’re completely comfortable with the potential loss of a device.

Mobile Platform Trends

The changing of the guard is under way. According to ComScore, a marketing intelligence firm, as of July, Google Android had almost 42% of the U.S. smartphone market and 22% of the EU market. Each quarter Google seems to jump several percentage points. In the United States, Android is consuming RIM’s market, while in the European Union, it’s replacing Symbian, to Nokia’s detriment. For example, in the most recent quarter, Google in-

Figure 3

Lack of Access to Mobile Productivity Activities: Impact on Employees



Note: Mean average ratings
Base: 323 respondents in August 2011 and 307 in March 2010
Data: InformationWeek Mobile Device Management and Security Survey of business technology professionals

R3321011/10

creased its EU share by about 16%, while Symbian simultaneously fell by the same amount. Next on the market-share list is Apple, with steady though modest overall increases in its 27% and 20% shares in U.S. and EU, respectively. Windows holds at around 6% for both. So RIM and Symbian are being marginal-

ized, which further emphasizes the need to centrally manage Android, iOS and to a lesser degree Microsoft devices while maintaining your BES capability if it’s needed. Now, compare that reality with Figure 4, which shows the breakdown among respondents at organizations with standardized mo-

FAST FACT

72%

allow Apple iOS devices
to access business
resources

bile platforms and IT-driven device and carrier selection.

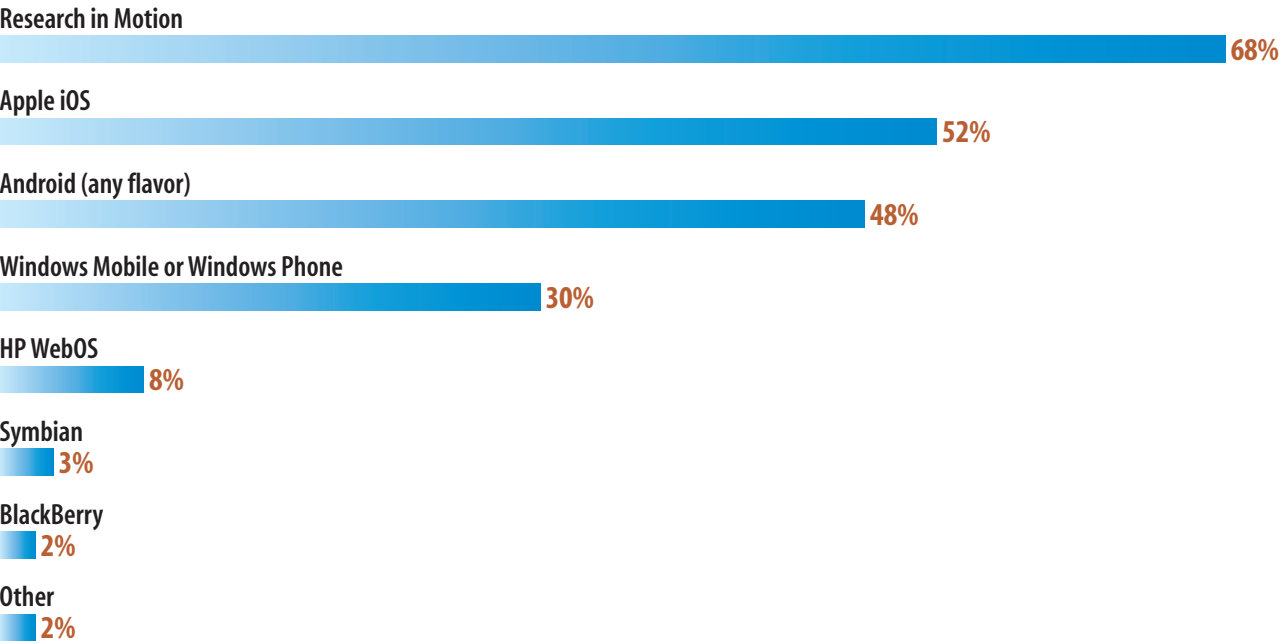
Clearly, the consumer label scares the heck out of many IT pros because we assume that these devices aren’t “enterprise-ready,” a term that implies security and manageability, while being utterly subjective since one person’s risk might not be another’s. Let’s say, for instance, you support a widely traveled team of researchers working in the oil and gas industry, toting valuable secrets on tablets, or attorneys working cases involving the exposure of personal health information and conversing with colleagues by email on smartphones. These companies have much to lose. On the flip side, your employees may be working with publicly available information of no particular sensitivity Even then, you need to be on top of security because many things can go wrong even in the most mundane of environments, whether it’s malware running amok from a rooted Droid device or a thief accessing the network via an iPhone VPN profile.

We asked our survey respondents about

Figure 4

Mobile Devices Selected by IT

What device type(s) has IT chosen?



Note: Multiple responses allowed

Base: 188 respondents at organizations with standardized mobile platforms and IT-driven device and carrier selection

Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/12

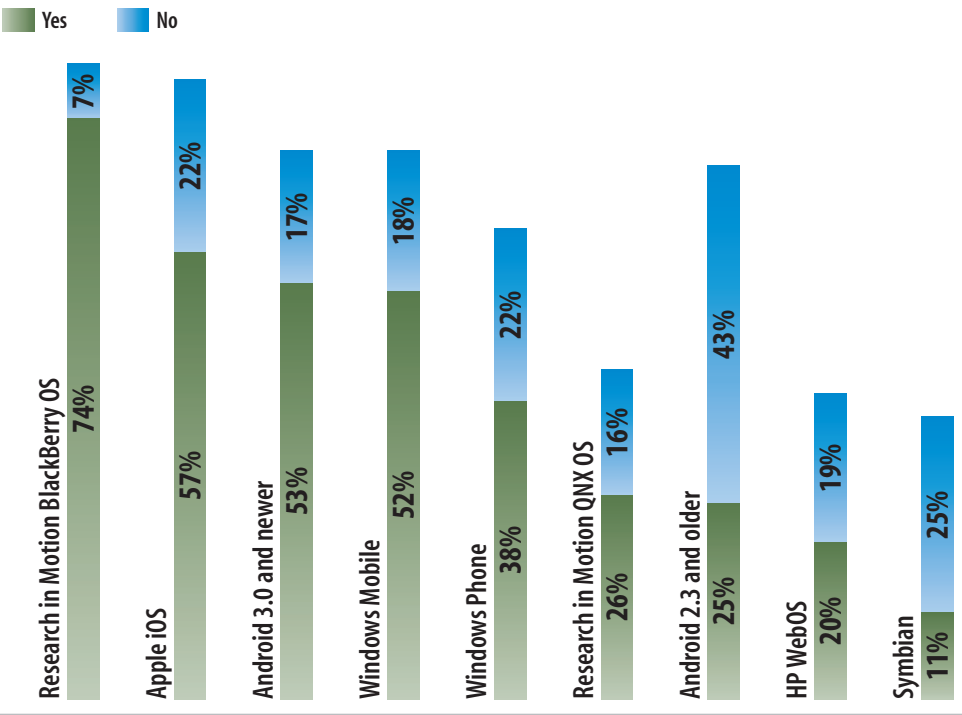
each platform’s ability to provide enterprise-ready support, defined as effective authentication, encryption and management controls; their answers are in Figure 5, next page.

We concede that this is a complex topic and one that’s constantly debated, even among infosec professionals. Also, finding succinct information on each platform’s or device’s ca-

Figure 5

Enterprise-Ready Mobile Platforms

We define “enterprise-ready” mobile platforms as those providing effective authentication, encryption and management controls that adequately protect business data. Do you consider the following mobile device operating systems enterprise-ready?



Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011 R3321011/17

pabilities can be difficult. However, we are mostly encouraged by our survey responses and find them pretty much in line with our own opinions.

For example, BlackBerry is the undisputed poster child for “enterprise class” because RIM baked in security a long time ago. The Apple iOS data-protection mechanisms that are part of the operating system utilize hardware-level crypto and a cohesive sandboxed application security architecture. According to the vendors we spoke with, iOS is enterprise class when consistently managed. Though Apple may not be ready for military-grade FIPS operation, the 22% who think it’s not manageable and secure are a bit off in our opinion.

Android, on the other hand, is all over the place on control and security and currently subpar compared with RIM and Apple. The

43% who say version 2.3 and older are not ready are right on. Android flavors vary widely, with versions prior to Honeycomb (pre-3.x)

having little to no built-in security. Erich Stuntebeck, a researcher for MDM provider AirWatch, says Droid vendors such as Motorola, HTC, Samsung and LG are forced to step up to the plate and each write security APIs for their versions of the OS since the “enterprise desired” functions aren’t native to the OS.

When managing devices, vendors like AirWatch have to keep track of which devices meet base levels for security and management. And to make matters worse, just because a device is running Honeycomb, which has security capabilities, doesn’t mean that the manufacturer has leveraged those capabilities for a certain model. Brian Reed, VP of products for mobile systems management company BoxTone, has a very similar view and says that his

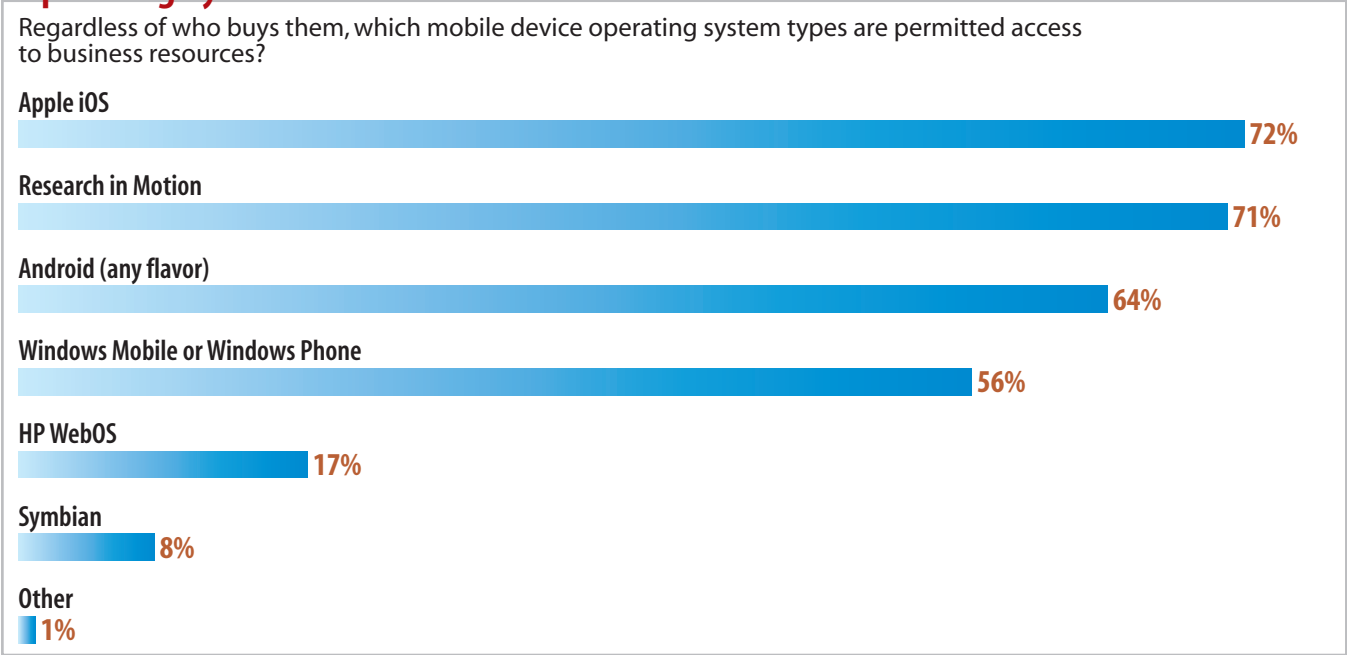
company advises customers to be selective when permitting Android devices into the managed fold. Devices not produced by the

larger manufacturers may not have the security mechanisms you want built-in.

Android’s enterprise security inconsistencies are beginning to turn for the better though. In October, a company called 3LM, comprised of ex-Googlers and poised to be absorbed by Google via its Motorola Mobility acquisition, announced standardized security extensions embedded within native Android OS. Tom Moss, CEO and co-founder of 3LM, says his company aims to catalyze enterprise adoption of Android by patching the main flavors of the core operating system from each of the main manufacturers. 3LM does this with a set of consistent hooks that can be used by MDM systems to alter and influence (currently) around 60 security policy settings. Interestingly enough, this software has been part of the main Android development lines since June, but it has only recently been activated. Several top-tier device and management vendors, including AirWatch, BoxTone, MobileIron and Motorola, are in the process of announcing support for the standardized 3LM Android control hooks, so that they will

Figure 6

Operating Systems Permitted to Access Business Resources



Note: Multiple responses allowed

Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/16

be usable by enterprises. We’ll be interested in seeing how this standardization is leveraged and whether the main manufacturers continue to write management APIs or rely on the common libraries developed by 3LM.

Several vendors we spoke with feel strongly

that Windows Phone needs time to mature and doesn’t yet have the built-in OS facilities to be considered enterprise ready. Though this may be a somewhat anecdotal observation, the current release does lack an encrypted file system, complex-password cap-

abilities and VPN connectivity. Microsoft certainly isn't standing still, though, and you can bet that upcoming releases, such as "Mango," will begin to address these short-falls. But because Microsoft is a bit behind, risk-averse organizations should probably pass, for now.

The takeaway idea here is that not all operating systems should be permitted to interact with corporate data, since some lack appropriate built-in management and security hooks. In the event that you deploy an

MDM to support multiple platforms, it's important to understand how candidate products reconcile security.

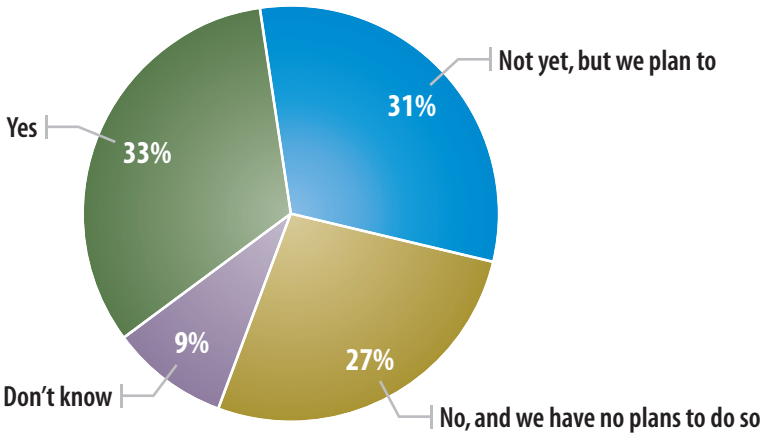
Mobile Apps

While we're discussing mobility, let's underscore a few key points. First, email and calendaring functions are still the key apps for mobile. Everyone uses them. Following second is the use of mobile Internet browsers

Figure 7

Custom Business Applications for Mobile Devices

Does your organization have plans to build and use custom business applications for mobile devices?



Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/7

for standard Web access, such as hitting news sites, researching a competitor's products or ordering something online. One of the main problems with using the browser for all types of application access is that screen real estate on smartphones is tiny, and many tablets aren't much better. Direct Web access doesn't always translate very

well. Therefore, many companies are either using third-party apps optimized for mobile devices or building their own to improve the user experience.

Our data shows serious interest in app development for iOS and Android, with the former being the leader at this time among respondents. We say "at this time" because

Some pundits are dubious about the long-term viability of VDI. We view this technology as a bridge.

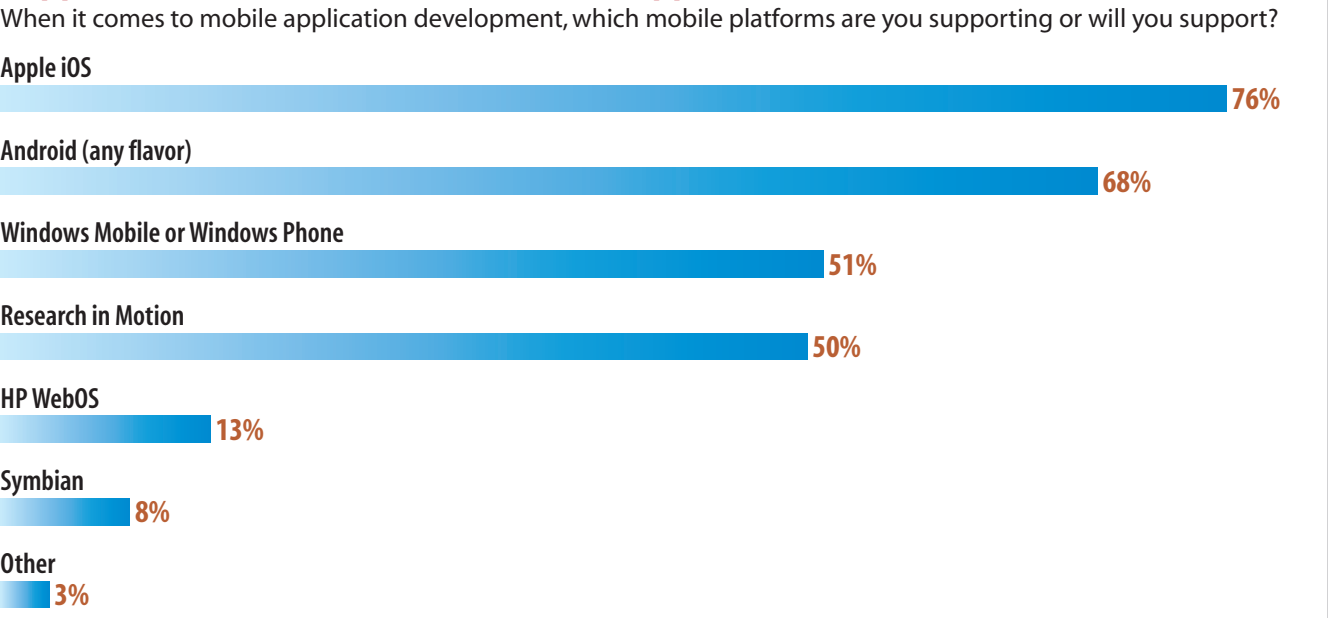
open platforms like Android are attractive to developers thanks to their inherent flexibility and lack of constraints, since Big Brother isn't screening your stuff. It will be interesting to see how these numbers morph over time.

Whether we're talking public-cloud SaaS apps, such as Google Docs or Salesforce, or a private app your organization builds for internal use, this is where the cutting-edge action is. For example, we've seen highly specialized sales apps built for the pharmaceutical industry that marry compelling graphics and CRM components onto tablets. It's a perfect form factor for reps who are in and out of meetings all day long. Tablet vendors want us to view these platforms as truly workable PC alternatives, and they can be in certain situations. Therefore we think it's pretty cool that app-based cloud services are of such interest to our respondents.

IT can control the types of apps permitted onto mobile devices by building a private app store via some MDM systems. Only your users can see and download from these stores, and what they see may well be based on their

Figure 8

Supported Mobile Platforms for Custom Applications



Note: Multiple responses allowed
Base: 208 respondents with plans to build and use custom business applications for mobile devices
Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/8

roles and applicable security policies. A private store is in order if you have internally developed line-of-business applications. You don't want to post these to the world via iTunes or the Android Market.

VMware, Citrix and Microsoft all offer vir-

tual desktop infrastructures to permit users to access desktop images over a network. Only the keyboard, mouse and screen updates travel back and forth between the user and the back end. Most VDI implementations require an active network connection, but

that’s changing, with some systems permitting a degree of off-line capability with a re-synchronization to the back end when the user is able to reconnect.

Some pundits are dubious about the long-term viability of VDI. We view this technology as a bridge between old and new, enabling the use of software built for traditional platforms on new devices. For example, health information system applications, in many cases, run only on very specific desktop builds—Windows XP SP3 with IE7 with Java version such and such and Adobe version this and that. Here, desktop virtualization makes perfect sense. By publishing these via VDI and extending their use to mobile platforms, IT can extend the useful life of critical applications while accommodating new workplace realities. VDI ties into MDM as just another app that’s permitted to be on the device with the corresponding enterprise profiles that contain authentication and VDI target server information. As with other apps, VDI profiles should be remotely removable, should a device leave the control of IT.

FAST FACT

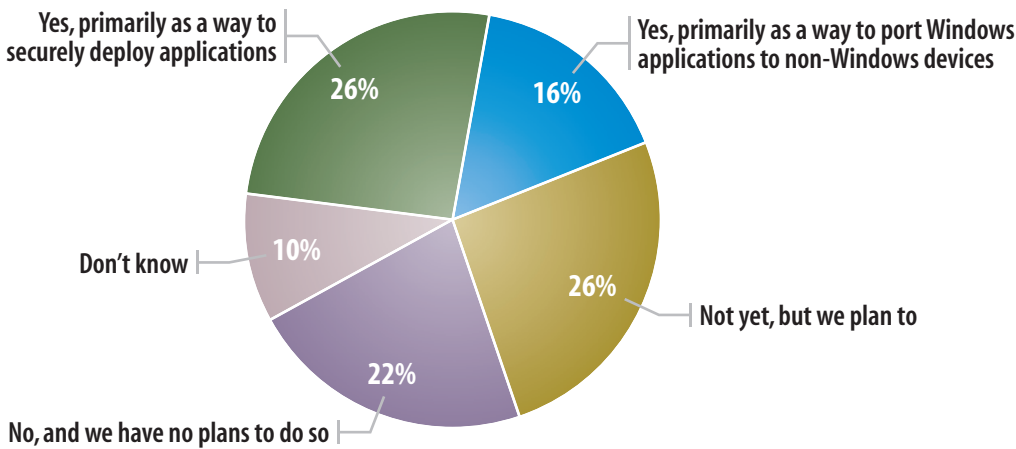
30%

give smartphones or tablets access to enterprise data by default

Figure 9

Use of Virtual Desktop Technologies Via Tablets

Do you use or plan to use virtual desktop technologies (terminal services, VDI, Citrix) via tablets?



Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/9

Mobile Device Policy

Our survey data shows an uptick in respondents placing mobile data security among their top priorities. That’s great. What’s not so good is taking the wrong approach—that is, to go tactical and dive right in, comparing a few MDM systems, buying one, and configur-

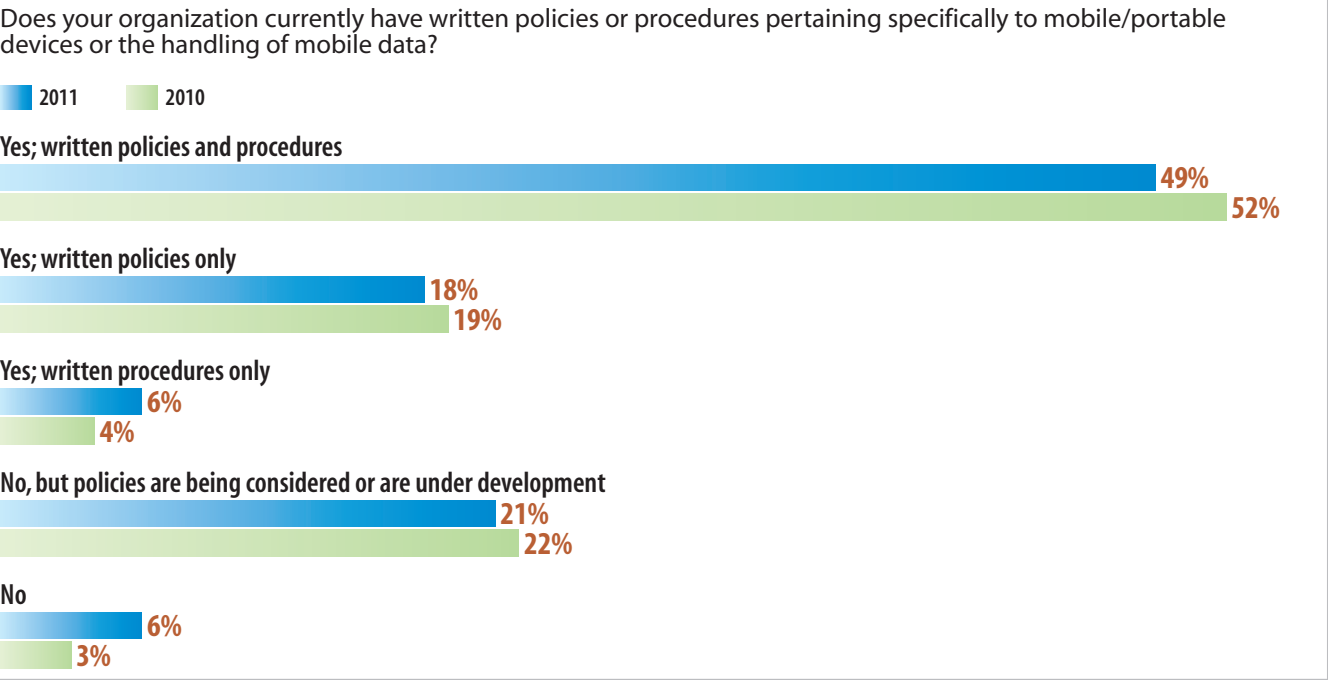
ing lockdown policies willy nilly. That will result in an employee revolt.

Better: Take a deep breath, step back and approach this strategically. Again referring to our 2011 Interop mobility session, we suggest these top-level steps for a successful integration of mobility policy:

- > Form a cross-functional mobility council comprised of IT, line-of-business leaders and a few users. The diversity of ideas will serve you well.
- > Prioritize goals and establish a mobility plan that defines what you want to accomplish with these devices. Take small steps, and open up functions as you begin to feel comfortable.
- > Determine the applications that can be used. Are we just talking email or is it that and more?
- > Determine your level of risk based on the type of data you process. Higher-risk data should translate into stricter policies.
- > Make your plan part of policy approved by business leadership.
- > Define the mobility policy in writing.
- > Document an end user license agreement, and have users sign it.
- > Define who pays for the device and data plan; expensing monthly can end up costing more than a flat stipend based on role.
- > Establish data security and management controls.

Figure 10

Mobile Device and Data Polices?



Base: 323 respondents in August 2011 and 307 in March 2010
Data: InformationWeek Mobile Device Management and Security Survey of business technology professionals

R3321011/19

> Enforce your written policies with MDM controls.
Security folks are always harping about policy, but trust us, it's a good idea to define in writing how your mobility strategy is going

to work. Once you know what you want to accomplish (because you've done your homework) putting it into action using one or more tactical security controls becomes much easier.

In addition to your own research and reasoning, we suggest tasking candidate MDM vendors with providing specific input on approaches to handling each phase of the device life cycle—from purchase to enrollment to operation to disposal. Another source for mobility policy ideas can be found at the Enterprise Mobility Foundation; its *Enterprise Mobility Policy Guidebook* is very thorough.

Security Control

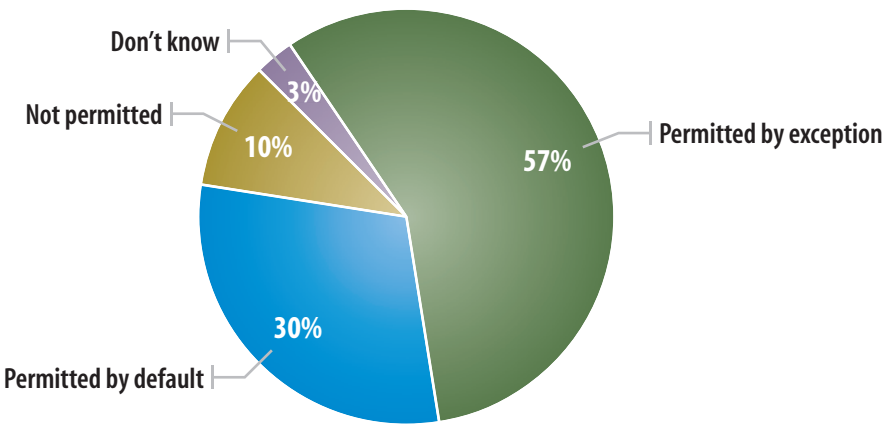
It's intuitively obvious that a mobile device, especially one with enterprise data on it, in the wrong hands isn't a good thing. So as pressure grows for organizations to supply workers with smartphones and tablets, partially or fully subsidize their purchase, or simply permit access to employee-owned devices, security controls in some form will be needed.

Organizations permitting data interaction by default are playing a risky game because if there are no settings—even basic ones—you rely on the user to implement the available controls, with the device passcode/PIN

Figure 11

Enterprise Data Access Via Mobile Device: Default vs. Exception

Are smartphones or tablets permitted access to enterprise data by default or by exception?



Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/15

being the most basic, and perhaps the most important. Take the worst-case scenario of a CEO who refuses to use a PIN to authenticate himself to his device. In the case of iOS, for example, a lack of PIN (or pass phrase, if you prefer) means that in the data at rest, crypto is not enabled. Our stubborn CEO who is too

busy to input a PIN also has the quarterly financial spreadsheets in his inbox in emails from the CFO.

Organizations we work with that have thought through mobility policy issues don't permit access by default. With the popularity of Microsoft Exchange as a back-end email



Related Report

In this report, How to Ensure 'Mobility' Translates to 'Agility,' we'll explain exactly how to harness mobile technologies to enhance and improve the processes on which your business relies—critical unless you want to end up trailing the competition.

FAST FACT

21%

use or plan to use MDM
in a SaaS model

system, Microsoft Exchange ActiveSync (EAS) was developed to permit a variety of phone platforms to receive “direct pushed” email, scheduling, contacts and tasks over secure SSL. When a user’s account is enabled for ActiveSync—meaning that supported mobile devices are permitted to be the end device—the user can access his data. As part of this process, the administrator can set device policies to lock down certain functions. ActiveSync is the most common mobile device manager, but it touches only the most basic of basic policy types, and these will vary by the version of ActiveSync you use and the mobile device. Though rudimentary, ActiveSync can permit administrators to set policies for remote full-device wiping, enforce device password and minimum password length, require alphanumeric or complex passwords, and set inactivity time lockouts.

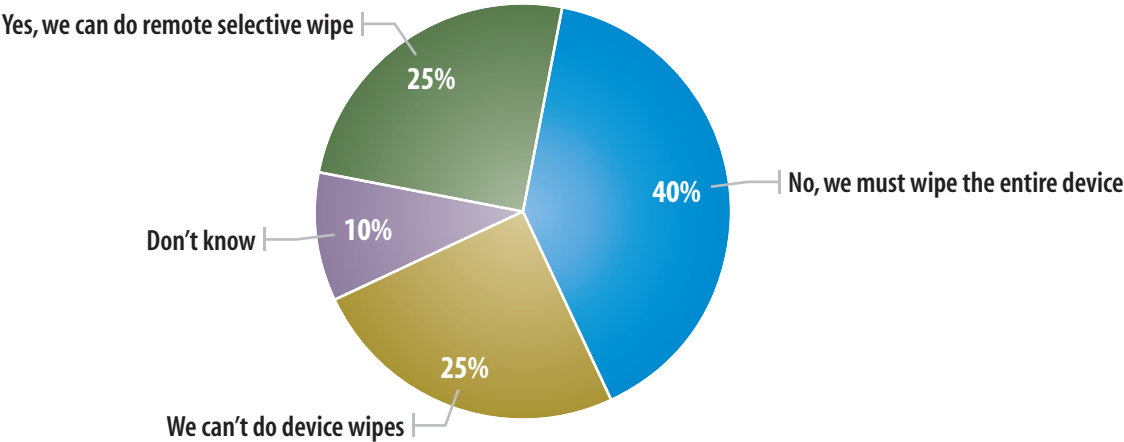
But ActiveSync offers very little outside of these basic functions. For more granular control, you need an MDM platform.

Full device wipes must be used with extreme care, especially when it comes to per-

Figure 12

Ability to Selectively Wipe Business Data From Personal Devices

If an employee uses a personal device to access business resources, do you have the ability to selectively wipe (delete) business-related data while leaving personal data intact?



Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/20

sonally owned devices. Because ActiveSync permits a managed device to be wiped, overzealous administrators can very easily remove both personal and enterprise access during a standard HR procedure that goes into motion after an employee is terminated. Or maybe there isn’t a procedure and the ad-

ministrator simply takes it upon herself to do it because it seems like a good idea. But what if the ex-employee owns that phone and doesn’t have a backup of his data? Is the company now liable for the loss? We highly recommend that you take the time to understand how MDM systems that interest you

carry out partial wipes, to remove enterprise digital certificates, email and VPN profiles, enterprise-specific apps, and other corporate data while leaving personal files intact.

Figure 13 lists a variety of security controls and features our respondents generally believe are of interest. It certainly seems by looking at the percentages that *everything* is of interest, and we can't blame respondents for saying, "yes, yes, OK, yes, that too," because most of it is pretty important.

When it comes time to decide which controls to implement, though, it's likely that the decision will be made on a platform-by-platform basis.

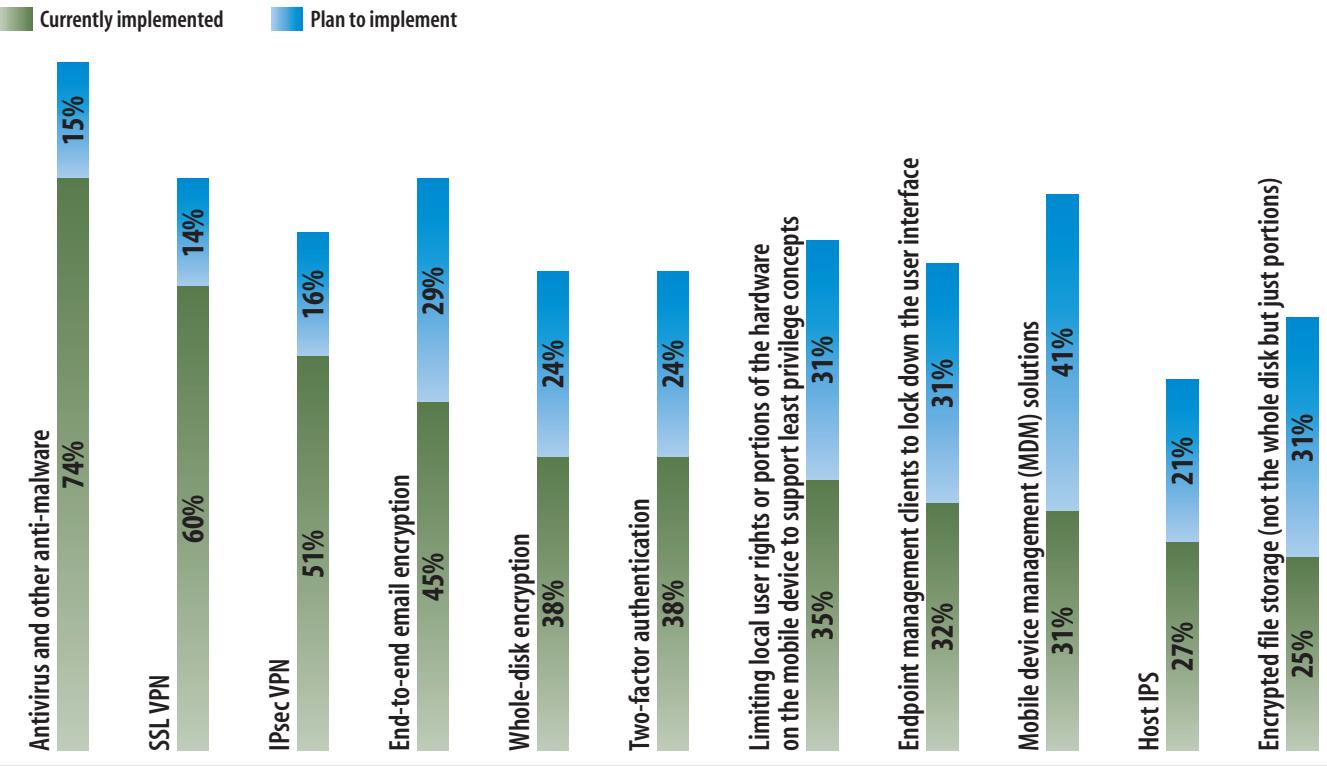
Cohesive Management Via MDM

"After feeling comfortable with RIM's BES for some time, it is now showing its age," says one respondent. "MDM vendors need to step up to the plate and offer device-agnostic granular security control while allowing the company and the end user to treat personal and corporate data separately. It might be a tall order, but it's badly needed."

Figure 13

Portable Device Security Controls

What security controls have you implemented or do you plan to implement within 12 months for protecting portable devices, including laptops, netbooks, tablets and smartphones?



Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/21

Very true, and in fact, security is the overriding objective for device management in general, and many agree that ActiveSync just isn't

enough to get that job done. It's too coarse and has too few control knobs. As we've discussed, it's no longer a BlackBerry-only world,

and OS/platform fragmentation makes effective risk reduction and management just about impossible without a multiplatform, full-featured MDM system.

In our report, *Dark Side of Mobile Apps: Keeping Data Safe on the Move*, we present data from our OS Wars survey data showing 343 respondents' top concerns with the growing number of mobile platforms. A good MDM system will, in our opinion, assuage at least the top four concerns, if not more.

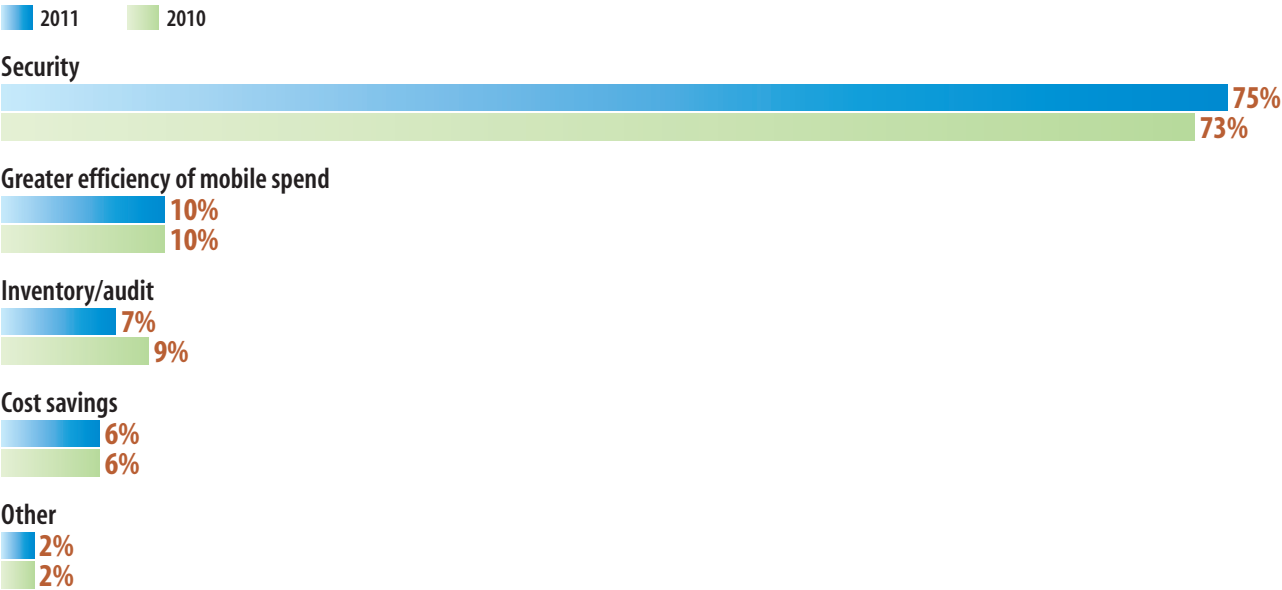
OK, so let's say you're ready to spend money on an MDM system to manage whatever comes down the road. Which one do you buy given the large number of vendors? Here are a few thoughts to ponder:

- > **How much** are you willing to spend per device per month? It's a competitive environment, and MDM vendors are likely in a deal-cutting mood because they want market share.
- > **Do you want a SaaS** or an on-premises model? For smaller organizations, SaaS may be perfect, while on-premises systems can often be provisioned as virtual

Figure 14

Primary Reason for Deploying MDM

What is the primary reason your organization deployed, or plans to deploy, a mobile device management (MDM) solution?



Base: 233 respondents in August 2011 and 192 in March 2010 at organizations using or planning to implement MDM
Data: InformationWeek Mobile Device Management and Security Survey of business technology professionals

R3321011/25

machines.

- > **Does the vendor** use gateway servers to deliver secure communications, somewhat like the BlackBerry and Good architectures use? If so, what role do these

gateways play in ensuring security and compliance? Do these gateways integrate with corporate-developed apps to provide better security for them?

- > **How many bells and whistles** do you

FAST FACT

25%

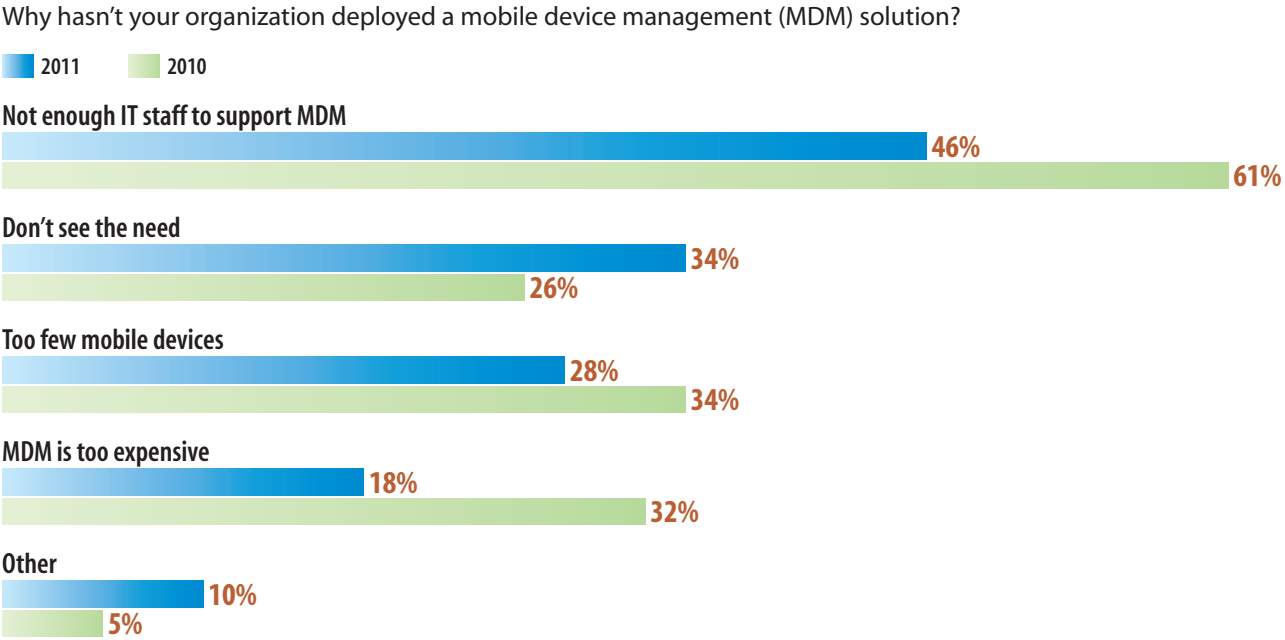
can do a remote selective wipe of business data on an employee's personal device

want? Is midlevel device management (a step above ActiveSync) good enough, or are you looking for that plus lots of device status and reporting capabilities? Some MDM systems label themselves as mobile systems managers, or MSMs, implying they control device security plus provides lots of device metrics, such as calling time, data consumption and more. That's just marketing.

- > **Do you need controls** for international travelers so you're not getting stuck with \$1,000 data bills?
- > **Which vendors** use device agents on which platforms? Some eschew agents and instead track mobile device status using the back-end infrastructure. Be sure to understand what infrastructure modifications are needed to accomplish this.
- > **Does the system support** partial wiping? Again, this is very important for shops that permit "bring your own device."
- > **Do you need** military-grade crypto and FIPS-certified software? If so, you may need to use a system, such as that from

Figure 15

Reasons for Not Deploying MDM



Note: Multiple responses allowed
Base: 90 respondents in August 2011 and 110 in March 2010 who have not implemented or have no plans to implement MDM
Data: InformationWeek Mobile Device Management and Security Survey of business technology professionals

- Good Technology, that specializes in hardened cryptographic sandboxes.
- > **Do you want to** remotely control devices, or back them up remotely?
 - > **Are you looking for** geolocation tracking

and other functions based on location? For example, the CFO's phone turned up in the hinterlands of Asia. Maybe we should wipe it completely, even though she owns it. Or we want to automatically

disable the camera on all phones that come within 300 feet of any corporate office building worldwide in order to prevent data theft via the camera.

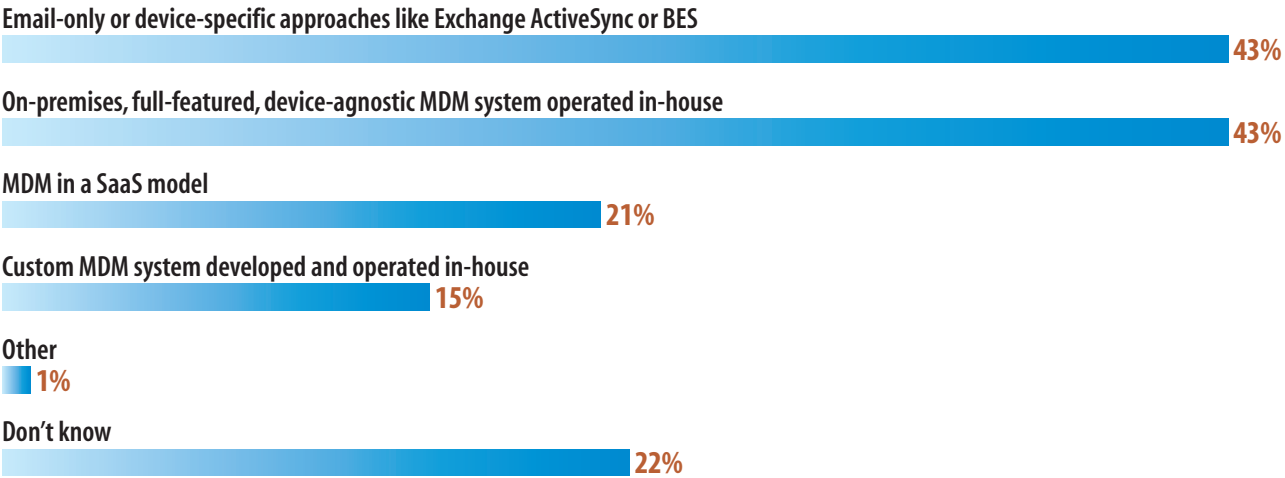
BoxTone’s Reed underscores the company’s focus on regulatory compliance, a top concern for respondents. “Proof of controls and separation of duties are very important in regulated industries,” he says. “Identifying which policies a user had at a particular point in time is highly important for security and the audit process.” As with some other vendors, BoxTone drives policy via the authentication process. The policy role you inherit is based on your group membership. It’s easy to tell which devices are in or out of compliance at any point in time. BoxTone also offers granular device controls, clientless iOS, some support for BES and an Android agent.

Alan Dabbieri, chairman of AirWatch, demonstrated the company’s self-provisioning process. We saw profiles for enterprise Exchange email and VPN appear along with a variety of authentication and encryption certificates and corporate documents that were

Figure 16

MDM Architecture

What MDM architecture(s) do you use or plan to use?



Note: Multiple responses allowed

Base: 233 respondents at organizations using or planning to implement MDM

Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/26

defined as part of the profile. Then we visited the private app store and pulled down an app pushed to us by our role membership. These apps may be ones you developed in-house and don’t want to put on iTunes or the Android Market, or they might be an anti-malware package for Android. To illustrate a partial wipe, a few clicks on the MDM console and

all of these corporate items simply disappeared off the device, leaving all personal items intact. AirWatch handles the major platforms and can act as a manager of managers for BES by controlling a subset of common policies. AirWatch’s secure email gateway is an optional component that adds another security layer and authenticates incoming devices

using UDID numbers and certificates.

Sean Ginevan of MobileIron adds that a company’s governance strategy is critical for successfully deploying and running MDM. This is another nod to looking before leaping—meaning don’t just buy any old product. Instead, think about what you need using the aforementioned cross-functional mobility steering committee, look how various offerings fit with your goals, and only then think about a purchase. MobileIron excels at evaluating a device’s security posture, and when it exceeds preset bounds, the user is cut off from the enterprise goods. Various actions will elicit different responses. Root your device, and it might get wiped. Install a prohibited app, and you may simply get a message telling you the app isn’t approved and by uninstalling it you will once again be able to access email. Uninstall it, and you’re back in business. Ginevan says that MobileIron believes that succinct user identity is important in order to classify the user’s role and thus provide the correct policy. The higher the risk, generally the more strict the re-



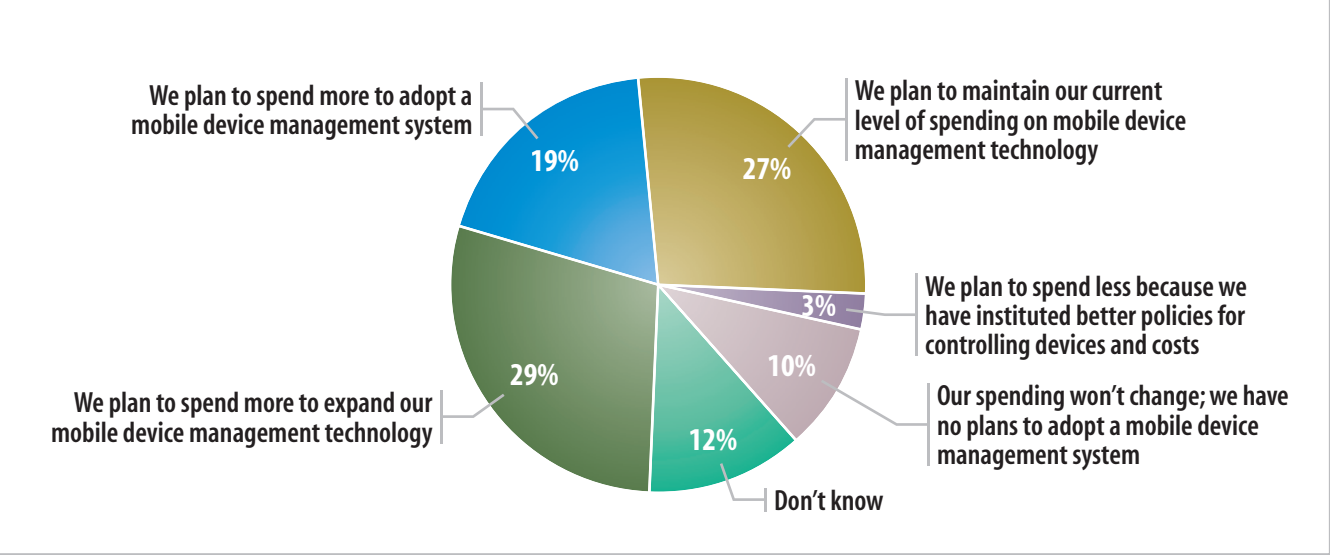
Related Report

Gone are the days when smart-phones were corporate-provided assets and IT managers could dictate the device (typically a BlackBerry) and enforce policies to ensure total management and security for enterprise data. Now what? Find out in this report, Surviving The ‘BYOD’ Revolution.

Figure 17

MDM Spending Plans

How will your mobile device management spending change in the next 12 months?



Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/28

sponse. The company also makes extensive use of certs to reduce the need for passwords and the support calls that go along with them.

Our recommendations for selecting an MDM platform break down into seven areas:
> **Breadth of platforms:** Support for multi-

ple platforms is a must. It must do iOS and Android. A link to RIM’s BES is desirable. Microsoft support, though it may be limited because of the platform’s newness, should be an option.

> **Platform security and manageability differentiation:** The various mobile plat-

FAST FACT

48%

expect to spend more
to adopt or expand MDM
in the next 12 months

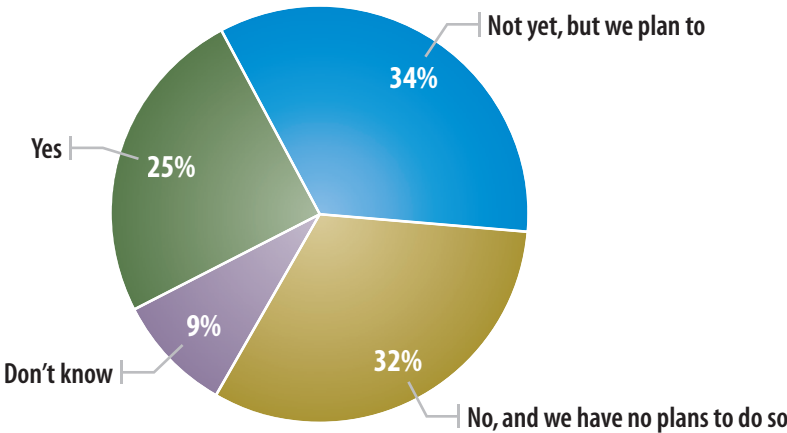
forms, and even the OS versions therein, are always going to offer different levels of assurance. Your MDM vendor needs to be able to help you understand on a continual basis what the relative risk is for allowing the use of iOS flavors vs. Android 2.x flavors vs. Android 3.x flavors vs. Microsoft. IT teams can't be expected to track all this.

- > **Control abstraction:** IT also shouldn't have to know the particulars of each individual platform. Instead, the MDM should abstract this and implement the desired controls under the hood.
- > **Directory integration:** Whenever possible, the mobile policy that's pushed to a user's device should be tied to a user's membership in a directory-based group (Microsoft Active Directory or similar). If a user is terminated and removed from the central directory, a typical HR process, this should initiate a partial wipe of enterprise data from the device.
- > **Self-service:** IT teams have too much on their plates as it is. Mechanisms for provi-

Figure 18

Access to Cloud Services Via Mobile Devices

Is your organization enabling access to cloud services or SaaS via mobile devices?



Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/5

sioning of devices via self-service portals are a big plus. Or, if users step over the bounds of a policy, such as installing a particular blacklisted app, the MDM should notify them of what they need to do to bring their devices back into compliance.

- > **Scalability and failover:** This is impor-

tant, particularly if you're running your own MDM system as opposed to a SaaS offering. In-house systems need to be up and running and servicing the communications that rely on them. Therefore, building in fault tolerance is important.

- > **Reporting:** If desired, the MDM vendor

should provide audit and compliance reporting as well as usage analytics and inventories.

All indicators in our survey point to increased MDM spending, but the trick is finding one that fits your budget and needs. What's not up for debate is that, in the face of new mobility demands, we need a plan to

handle platform upheaval before it spins further out of control—and prior to a career-halting security breach.

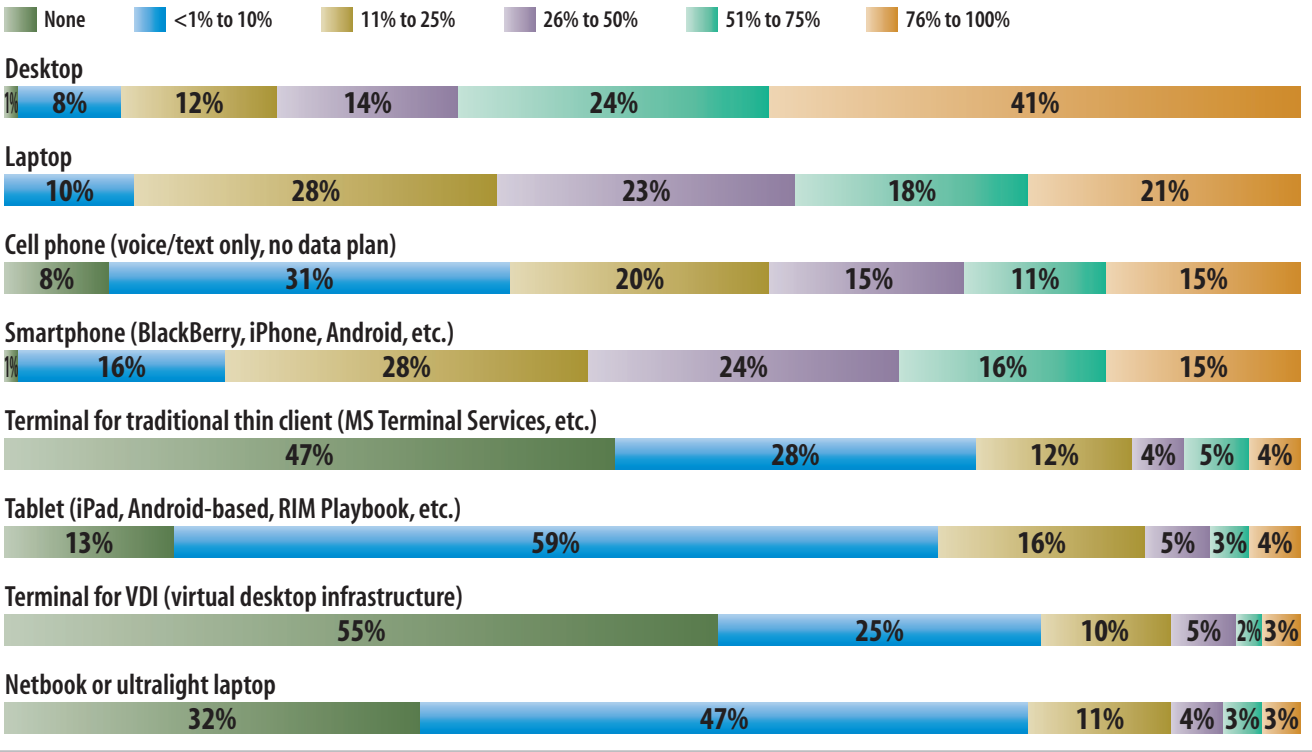
Before you buy any self-proclaimed miracle MDM cure, commit time and resources to defining how you envision smartphones and tablets interacting with your data. List the security controls you'd like to see, and then

come up with a rough idea of the procedures for provisioning, managing and disposing of devices. And don't do this in a vacuum. Form a mobility council comprised of IT, lines-of-business representatives and average users. Only then are you ready to match mobile device management system controls to your needs.

Figure 19

Percentage of Employees Using Devices

What percentage of your organization's employees use the following device types for business purposes, regardless of whether the device is personally or company owned?



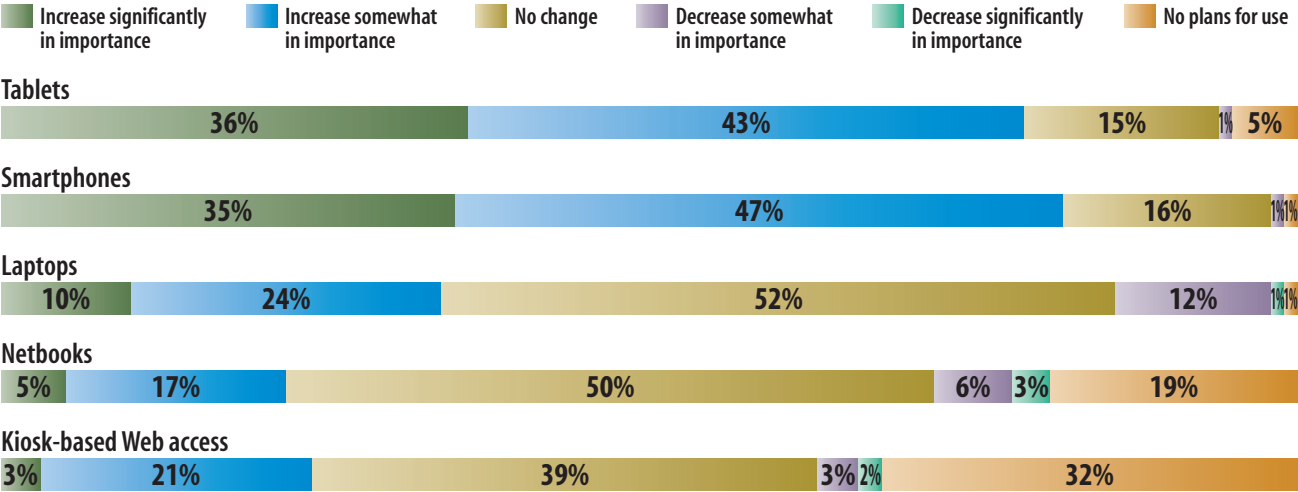
Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011 R3321011/1

APPENDIX

Figure 20

Mobile Technology Impact on Productivity

Thinking about the next 24 months, how critical a role will the following mobile technologies play in business productivity at your company?



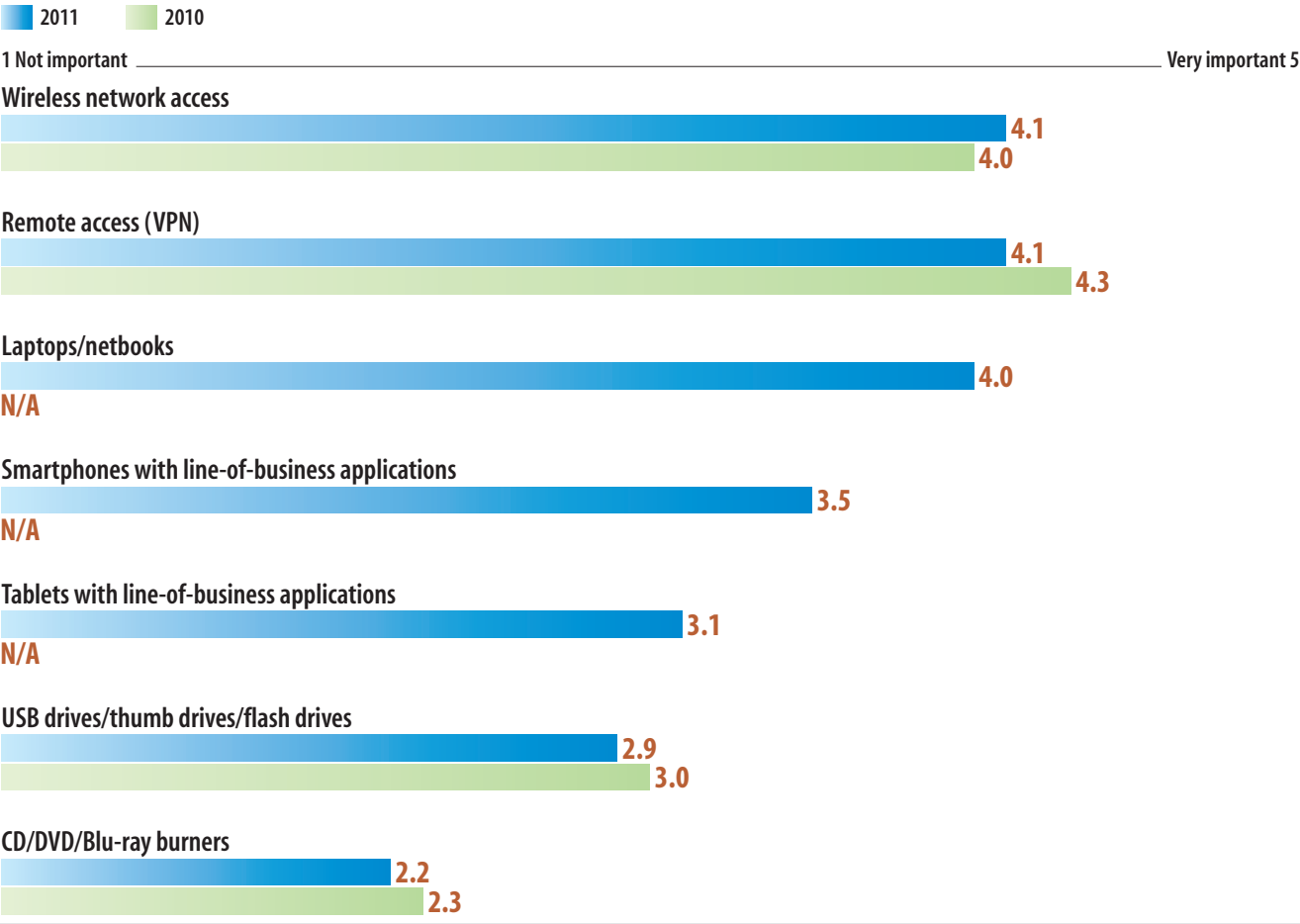
Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/2

Figure 21

Importance of Employee Access to Mobile Technologies

Using a scale of 1 to 5, where 1 is “not important” and 5 is “very important,” how important is it that employees are provided with the following technologies in support of their jobs?



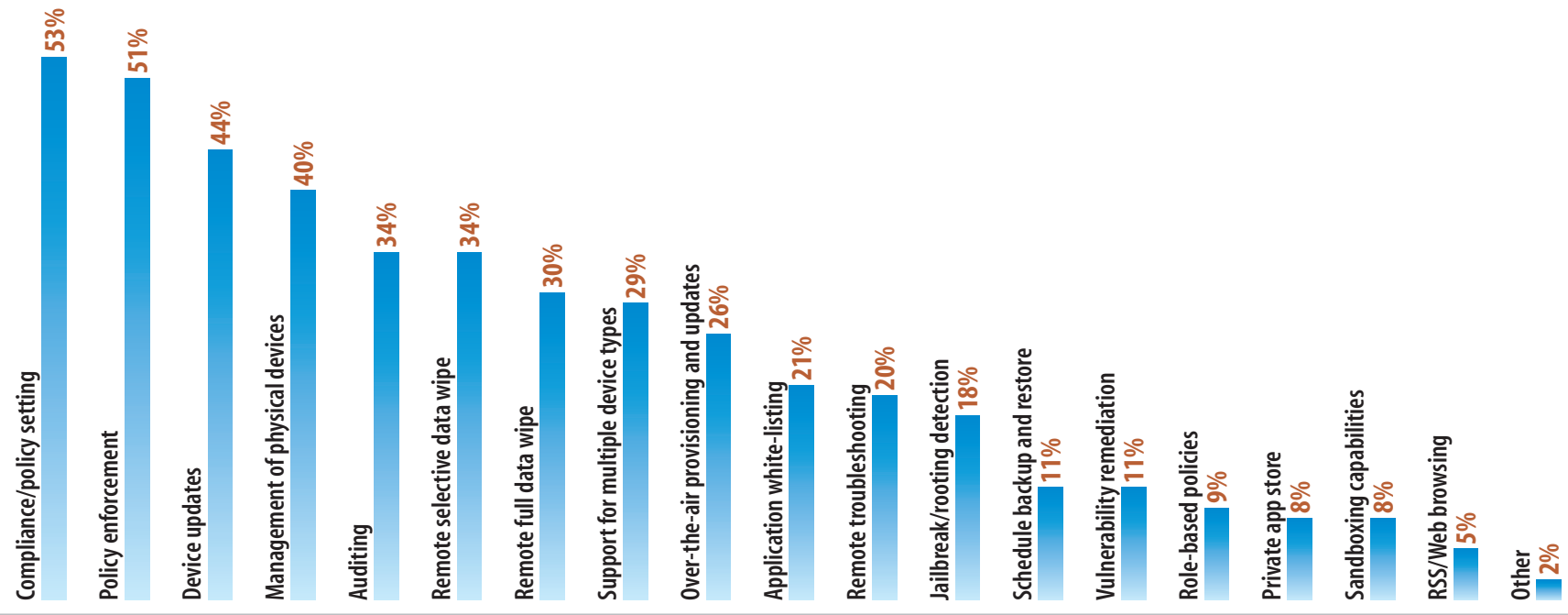
Note: Mean average ratings
Base: 323 respondents in August 2011 and 307 in March 2010
Data: InformationWeek Mobile Device Management and Security Survey of business technology professionals

R3321011/4

Figure 22

MDM Features of Interest

Whether or not you have a mobile device management (MDM) system for controlling tablets and smartphones, which centrally controlled features are of greatest interest to you?



Note: Five responses allowed

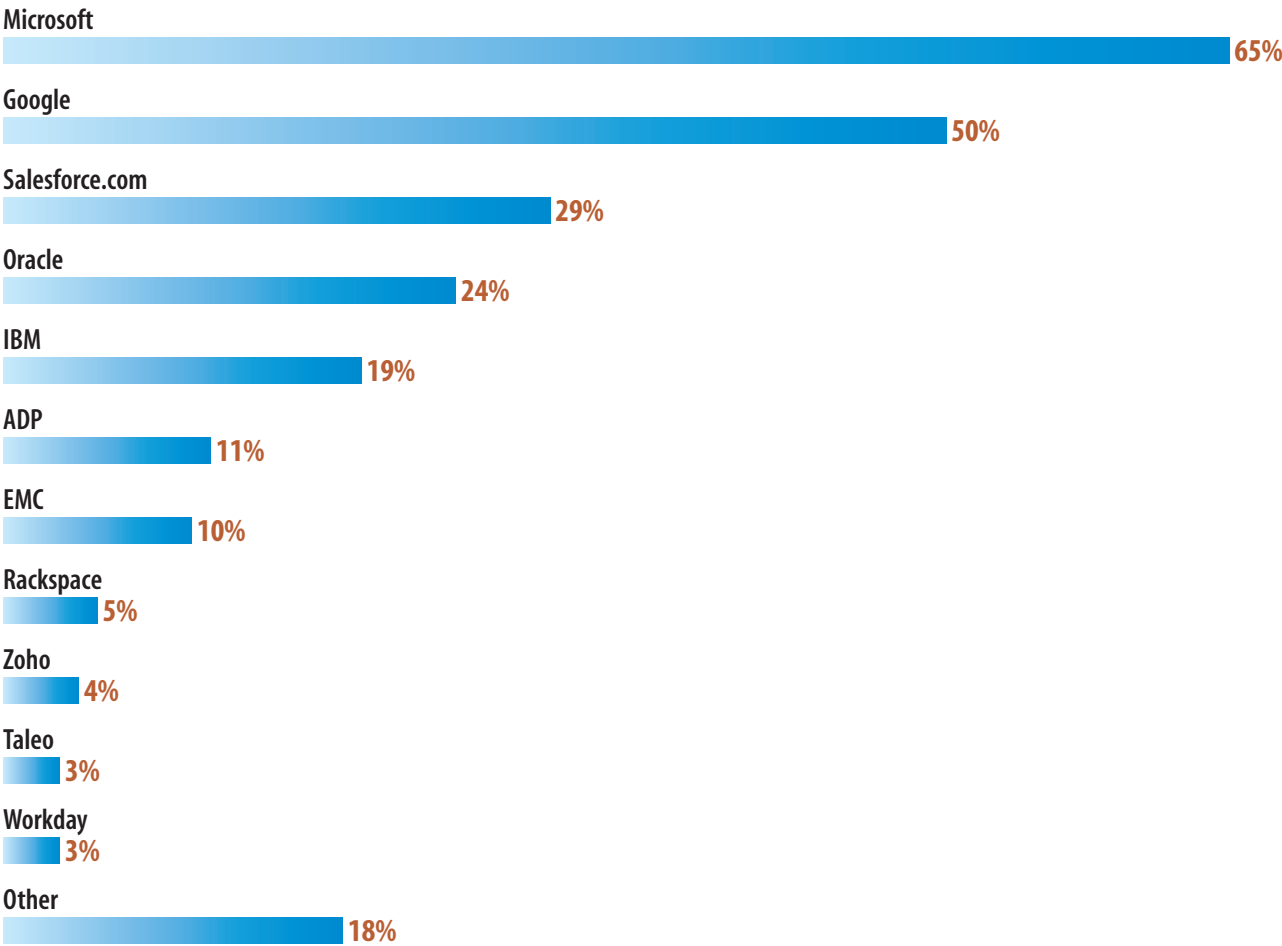
Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/27

Figure 23

Types of Cloud Services Accessible Via Mobile Devices

What cloud or SaaS services do, or will, you allow access to via mobile devices?



Note: Multiple responses allowed

Base: 185 respondents enabling access to cloud services or SaaS via mobile devices

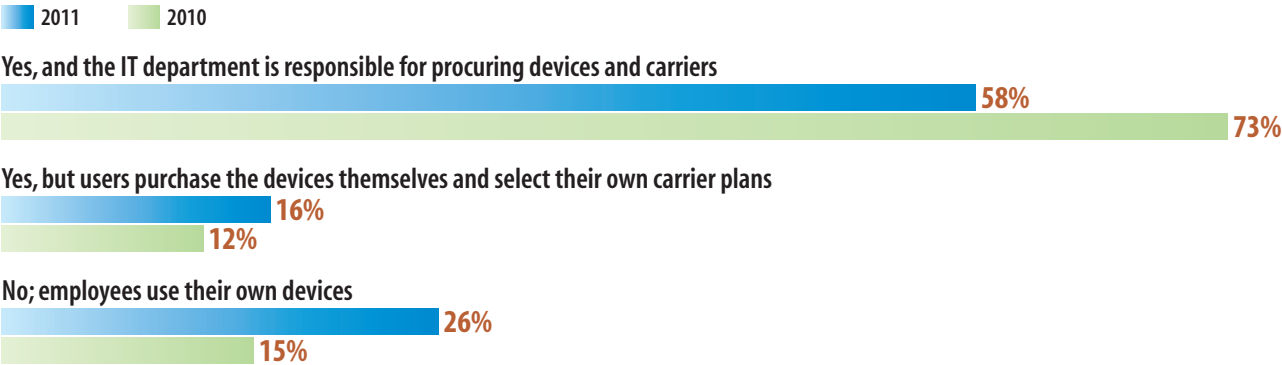
Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

RR3321011/6

Figure 24

Standardized on a Mobile Device Platform?

Has your organization standardized on a mobile device platform?



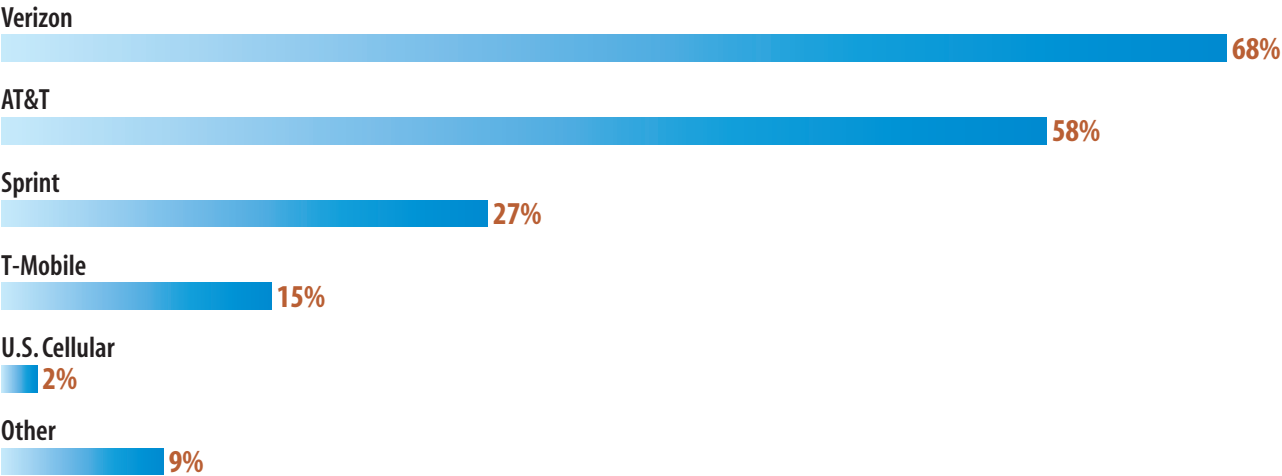
Base: 323 respondents in August 2011 and 307 in March 2010
Data: InformationWeek Mobile Device Management and Security Survey of business technology professionals

R3321011/11

Figure 25

Carriers Selected by IT

What carrier(s) has IT chosen?



Note: Multiple responses allowed

Base: 188 respondents at organizations with standardized mobile platforms and IT-driven device and carrier selection

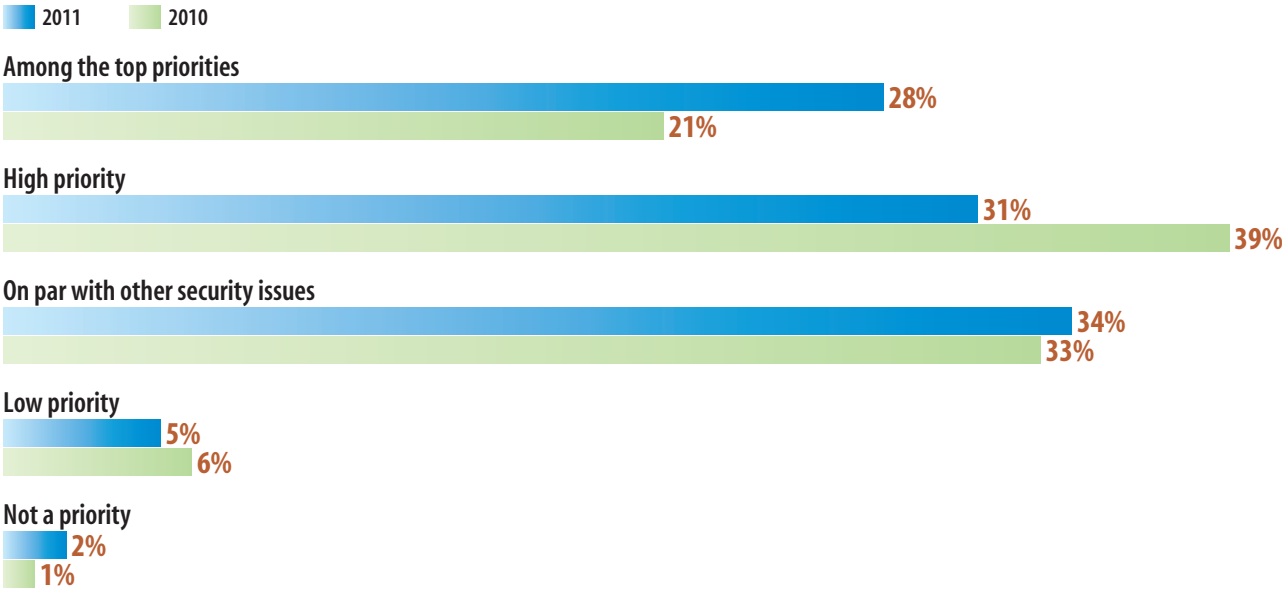
Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/13

Figure 26

Prioritization of Mobile Data Security

Relative to other information security issues, what priority is your organization placing on mobile data security?



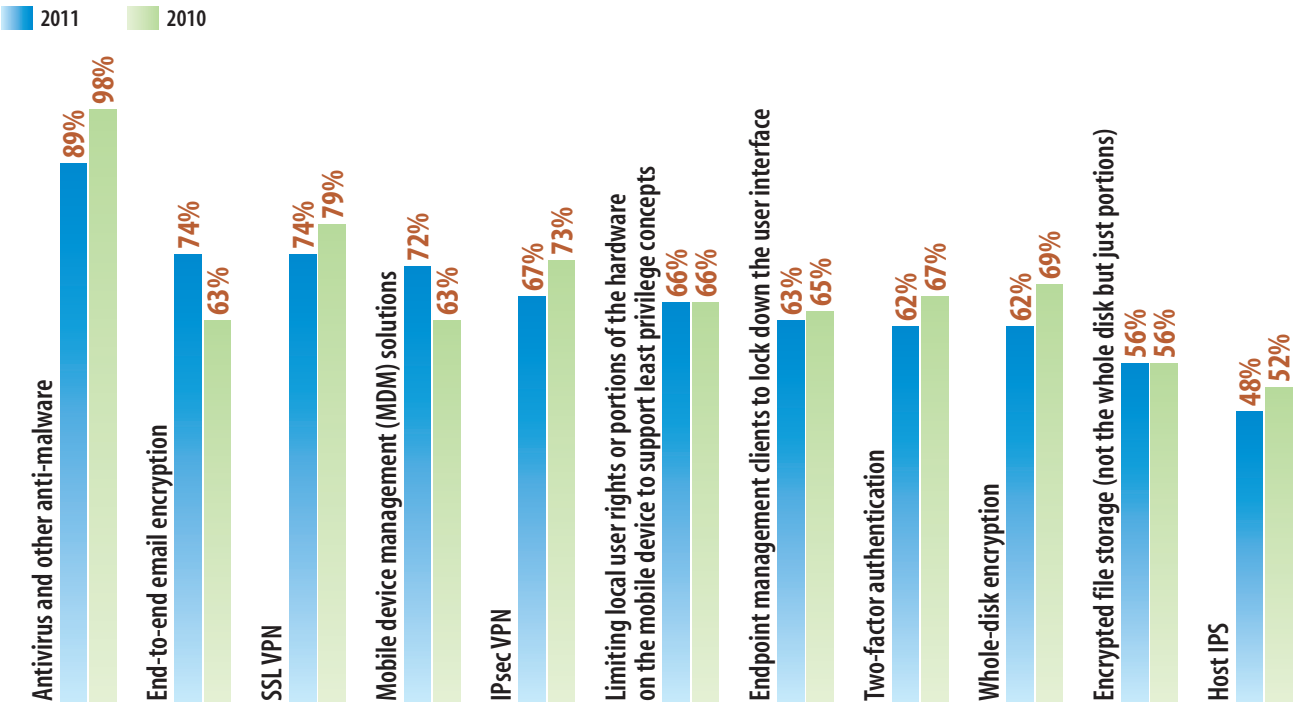
Base: 323 respondents in August 2011 and 307 in March 2010
Data: InformationWeek Mobile Device Management and Security Survey of business technology professionals

R3321011/18

Figure 27

Portable Device Security Controls: 2010 vs. 2011

What security controls have you implemented or do you plan to implement within 12 months for protecting portable devices, including laptops, netbooks, tablets and smartphones?



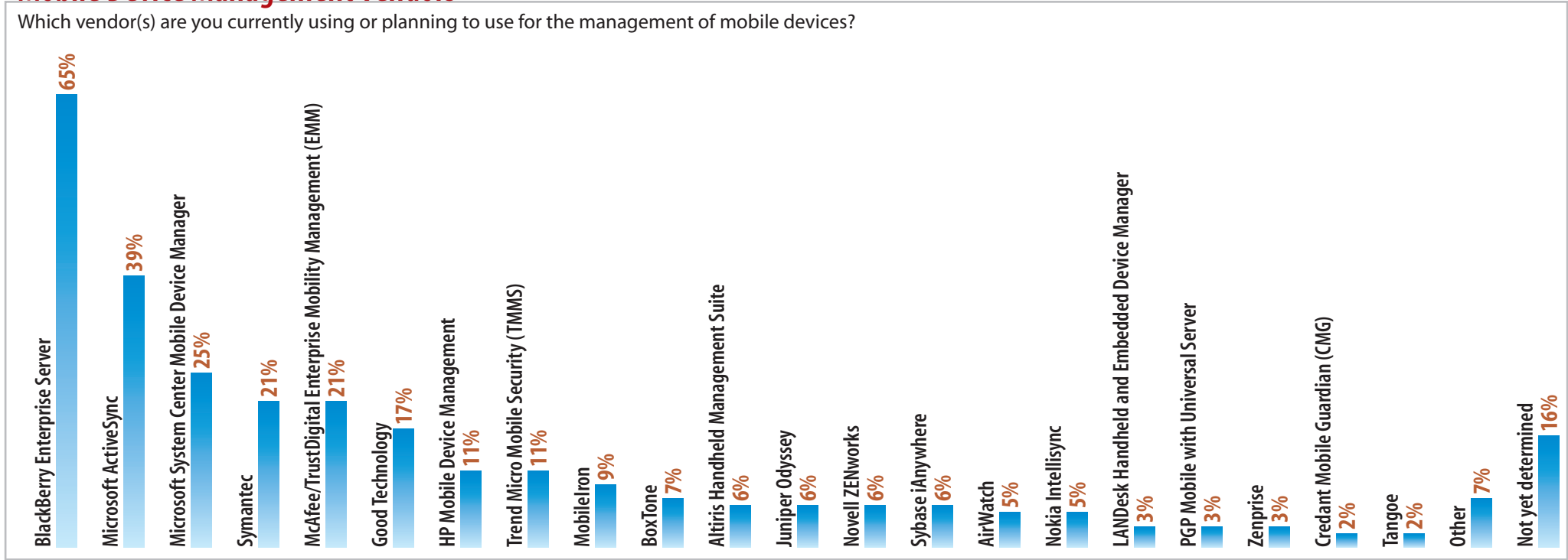
Note: Percentages reflect a response of “currently implemented” or “plan to implement”
Base: 323 respondents in August 2011 and 307 in March 2010
Data: InformationWeek Mobile Device Management and Security Survey of business technology professionals

R3321011/22

Figure 28

Mobile Device Management Vendors

Which vendor(s) are you currently using or planning to use for the management of mobile devices?



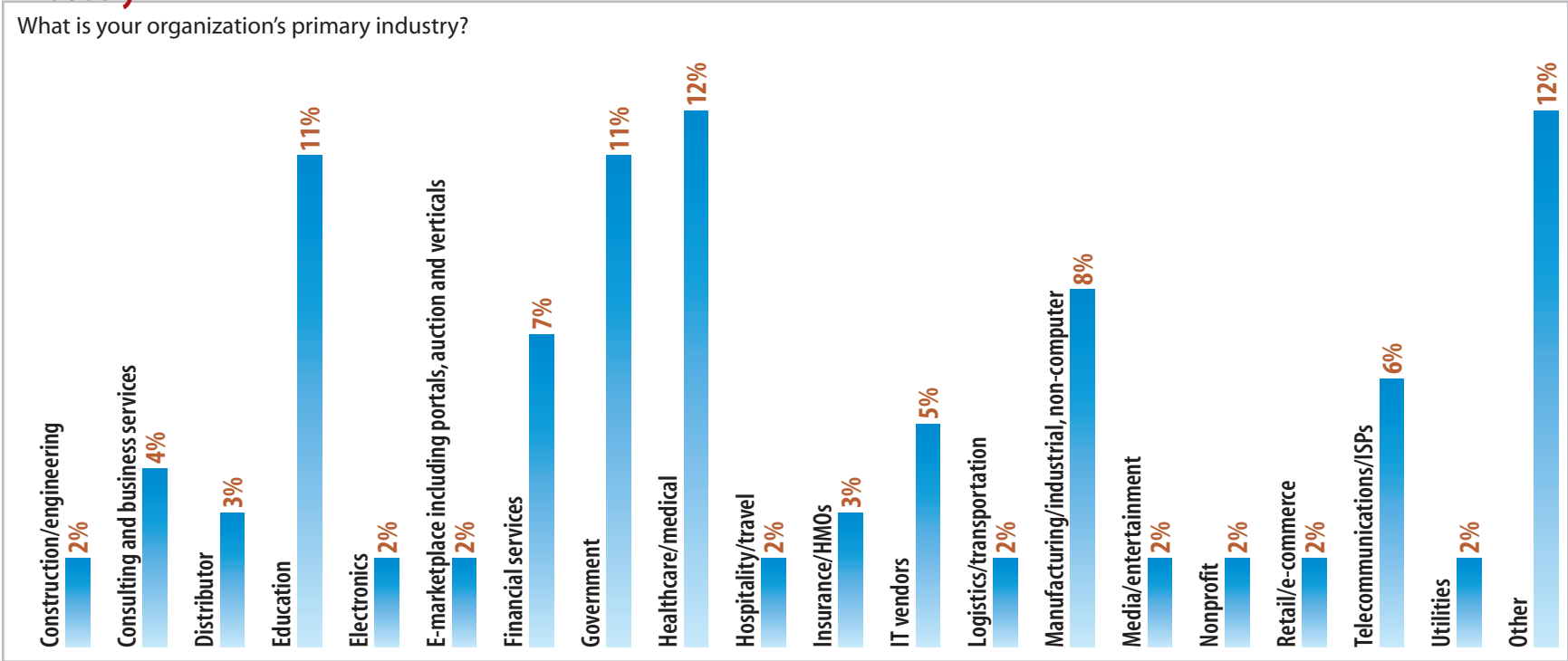
Note: Multiple responses allowed
Base: 233 respondents at organizations using or planning to implement MDM
Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/24

Figure 29

Industry

What is your organization's primary industry?



Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/31

Figure 30

Job Title

Which of the following best describes your job title?

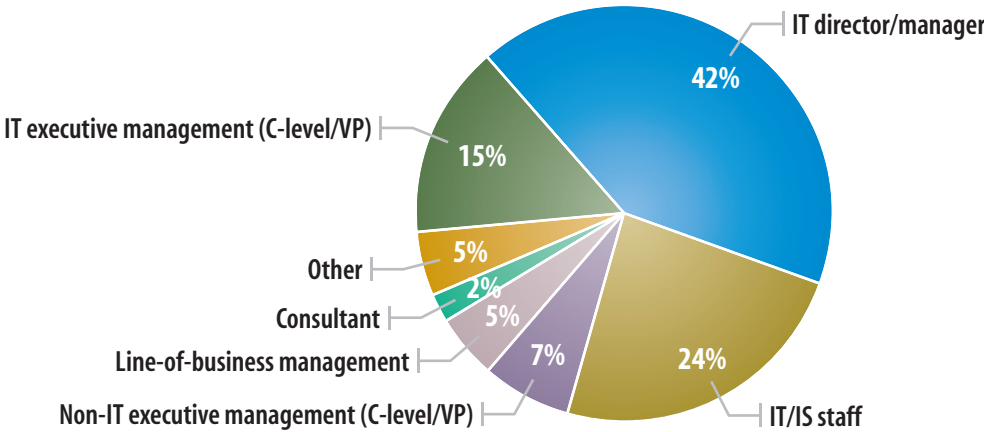
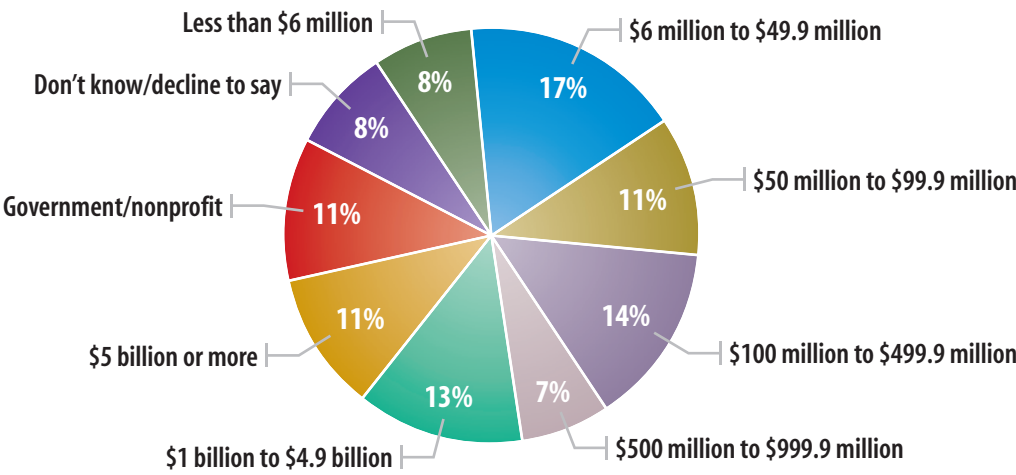


Figure 31

Company Revenue

Which of the following dollar ranges includes the annual revenue of your entire organization?



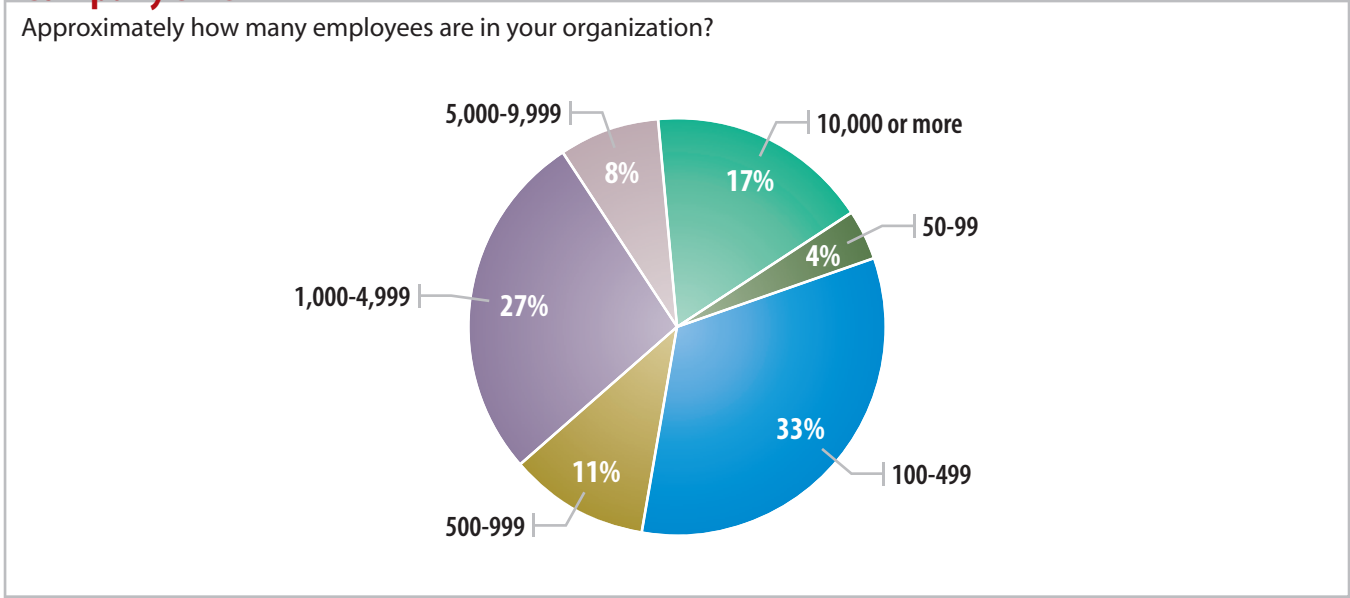
Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/30

Figure 32

Company Size

Approximately how many employees are in your organization?



Data: InformationWeek 2011 Mobile Device Management and Security Survey of 323 business technology professionals, August 2011

R3321011/32

MORE
LIKE THIS

Want More Like This?

Making the right technology choices is a challenge for IT teams everywhere. Whether it's sorting through vendor claims, justifying IT projects or implementing new systems, there's no substitute for experience. And that's what *InformationWeek* provides—analysis and advice from IT professionals. Our Reports site houses more than 900 reports and briefs, and more than 100 new reports are slated for release in 2012. Right now, you'll find:

Research: Wireless Nation 2011: Cutting the cord for employees and visitors is a matter of when, not if. Wi-Fi speeds now rival copper, and security advancements mean your data will be safe. There's no reason to wait.

Informed CIO: How to Ensure 'Mobility' Translates to 'Agility': Pervasive connectivity is no longer the future, it's the present, and organizations that rely on fixed communications mechanisms are limiting their potential. In this report, we'll explain how to harness mobile technologies to enhance and improve the processes on which your business relies.

Strategy: Surviving The 'BYOD' Revolution: End-user demands for a wider selection of smartphones and tablets—including the option to connect their own devices to the corporate network—are gaining traction. Gone are the days when smartphones were corporate-provided assets and IT managers could dictate the device and enforce policies to ensure total management and security for enterprise data. Now what?

PLUS: Find signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek 500* and the annual State of Security report; full issues; and much more.

Newsletter

Want to stay current on all new *InformationWeek Reports*? Subscribe to our weekly newsletter and never miss a beat.

[Subscribe](#)